# Swimming IoT:

## A hackers journey into the secrets of modern yacht (in)security

Industrial Cybersecurity 2018:
Opportunities and challenges in Digital Transformation

# Agenda

- Who am I
- Yachts and ships
- ICS in ships?
- attack vectors
- Bugs in maritime IT equipment

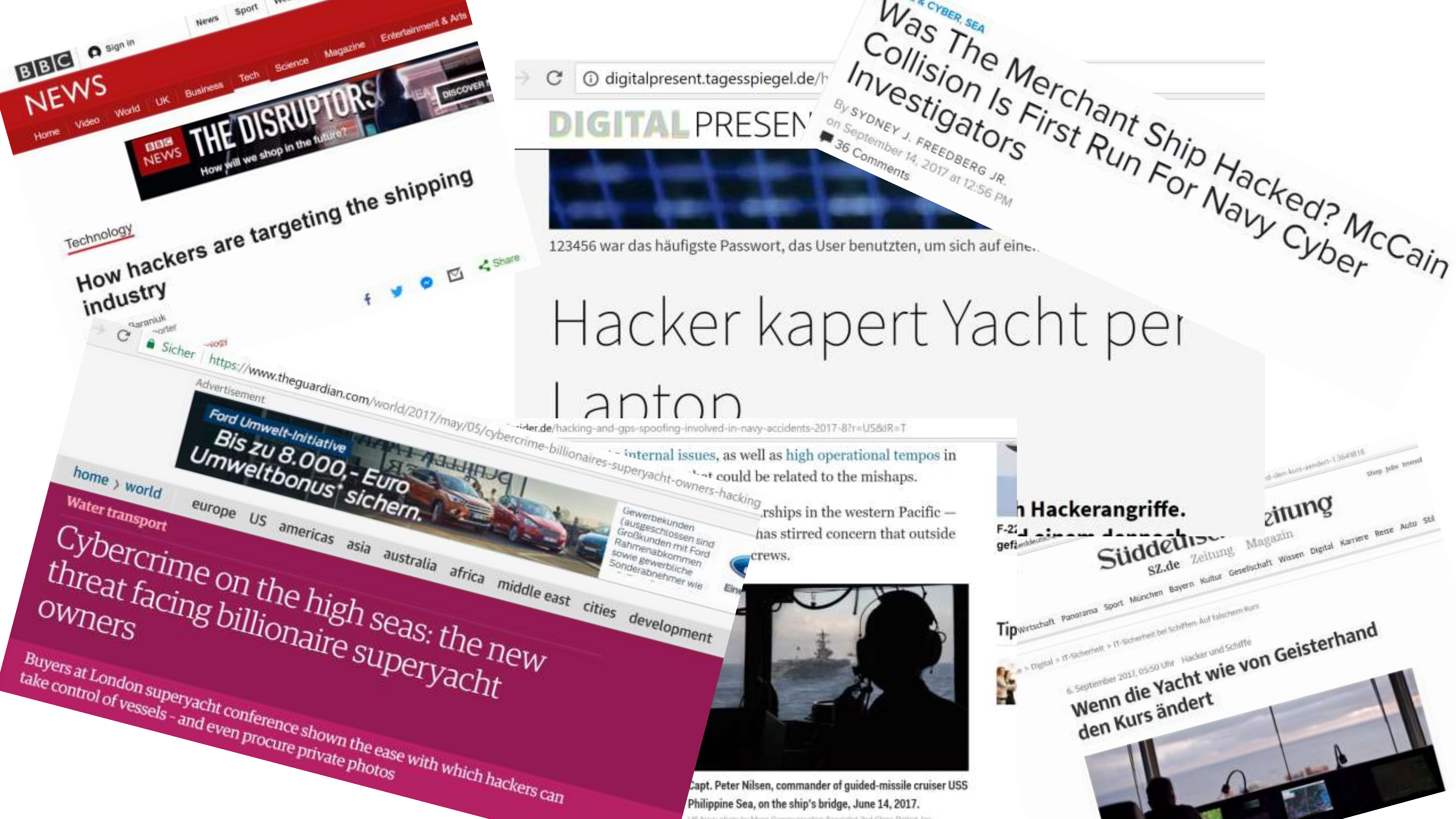
# Stephan Gerling @ObiWan666

I am older than the internet
Certified as “GCFA, CISSP, MCSE, CCNA, etc.”
Electronic Specialist,
several years German Aviation Army navigation system electronic specialist
More than 31 years a volunteer firefighter in my town
Security Evangelist @ROSEN-Group in Oil & Gas Industrie
and CERTivation, latest ROSEN Group Spin Off
I void warranties

- Geraffel
- IamTheCavalry

I am older than the internet
Certified as “GCFA, CISSP, MCSE, CCNA, etc.”
Electronic Specialist,
several years German Aviation Army navigation system electronic specialist
More than 31 years a volunteer firefighter in my town
Security Evangelist @ROSEN-Group in Oil & Gas Industrie
and CERTivation, latest ROSEN Group Spin Off
I void warranties

- Geraffel
- IamTheCavalry



BBC NEWS

Sign in

News Sport

Home Video World UK Business Tech Science Magazine Entertainment & Arts

BBC NEWS THE DISRUPTORS How will we shop in the future? DISCOVER

Technology

How hackers are targeting the shipping industry

Share

digitalpresent.tagesspiegel.de/h

DIGITAL PRESEN

123456 war das häufigste Passwort, das User benutzten, um sich auf eine

Hacker kapert Yacht per Laptop

& CYBER, SEA

Was The Merchant Ship Hacked? McCain Collision Is First Run For Navy Cyber Investigators

By SYDNEY J. FREEDBERG JR.
on September 14, 2017 at 12:56 PM

36 Comments

Sicher https://www.theguardian.com/world/2017/may/05/cybercrime-billionaires-superyacht-owners-hacking

Advertisement

Ford Umwelt-Initiative
Bis zu 8.000,- Euro Umweltbonus* sichern.

Gewerbekunden (ausgeschlossen sind Großkunden mit Ford Rahmenabkommen sowie gewerbliche Sonderabnehmer wie

home › world

europe US americas asia australia africa middle east cities development

Water transport

Cybercrime on the high seas: the new threat facing billionaire superyacht owners

Buyers at London superyacht conference shown the ease with which hackers can take control of vessels - and even procure private photos

sider.de/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8?r=US&IR=T

internal issues, as well as high operational tempos in … could be related to the mishaps.

…rships in the western Pacific — … has stirred concern that outside … crews.

Capt. Peter Nilsen, commander of guided-missile cruiser USS Philippine Sea, on the ship's bridge, June 14, 2017.

h Hackerangriffe.

Süddeutsche Zeitung
SZ.de Zeitung Magazin

Shop Jobs Immo

Wirtschaft Panorama Sport München Bayern Kultur Gesellschaft Wissen Digital Karriere Reise Auto Stil

Digital > IT-Sicherheit > IT-Sicherheit bei Schiffen: Auf falschem Kurs

6. September 2017, 05:50 Uhr Hacker und Schiffe

Wenn die Yacht wie von Geisterhand den Kurs ändert

# Accidents in 2017

| | |
|---|---|
| Februar: | Containervessel 10h without access to Navigationsystem |
| 18. Sep | Norwegian: GPS Jamming from eastern direction |

US Navy involved in 4 collisions in eastern pacific

| | |
|---|---|
| • Februar | USS Antietam in Bay of Tokios grounded |
| • Mai | USS Lake Champlain: collision with trawler |
| • 17. Juni | USS Fitzgerald: collision with freighter |
| • 21. August | USS John S. McCain: collision with Tanker |

# Vessels, Yachts and ships

## Overview

A **yacht** is a recreational boat or ship.

The term originates from the Dutch word jacht, which means "hunt"

It was originally defined as a light fast sailing vessel used by the Dutch navy to pursue pirates and other transgressors around and into the shallow waters of the Low Countries.

# Size matters

| | |
|---|---|
| Boot | up to 7m (20ft.) |
| Yacht | >= 10m (33 Fuß) |
| Super Yacht | bigger than 24m (79 ft.) |
| mega yacht | any yacht over 50 meters (164 ft.) |

# Superyacht

Indigo Star
Length 38,8m
Beam 7,7m

© Manuel Hernández
MarineTraffic.com

# Swimming IoT

Modern vessels becomme swimming IoT devices

- Vessel Traffic Service (VTS)
- Automatic identification system (AIS)
- Autopilot
- GPS
- Radar
- Camera‘s, including Thermal imaging
- Engine control and monitoring (some now cloud based)
- Internet Access
- Entertainmentsystems

# NMEA

NMEA 0183  (National Marine Electronics Association)

A combined electrical and data specification for communication between marine electronic devices, 4800 Baud speed

- echo sounder
- Sonars
- Anemometer
- Gyrocompass
- Autopilot
- GPS receivers

and many other types of instruments

# NMEA

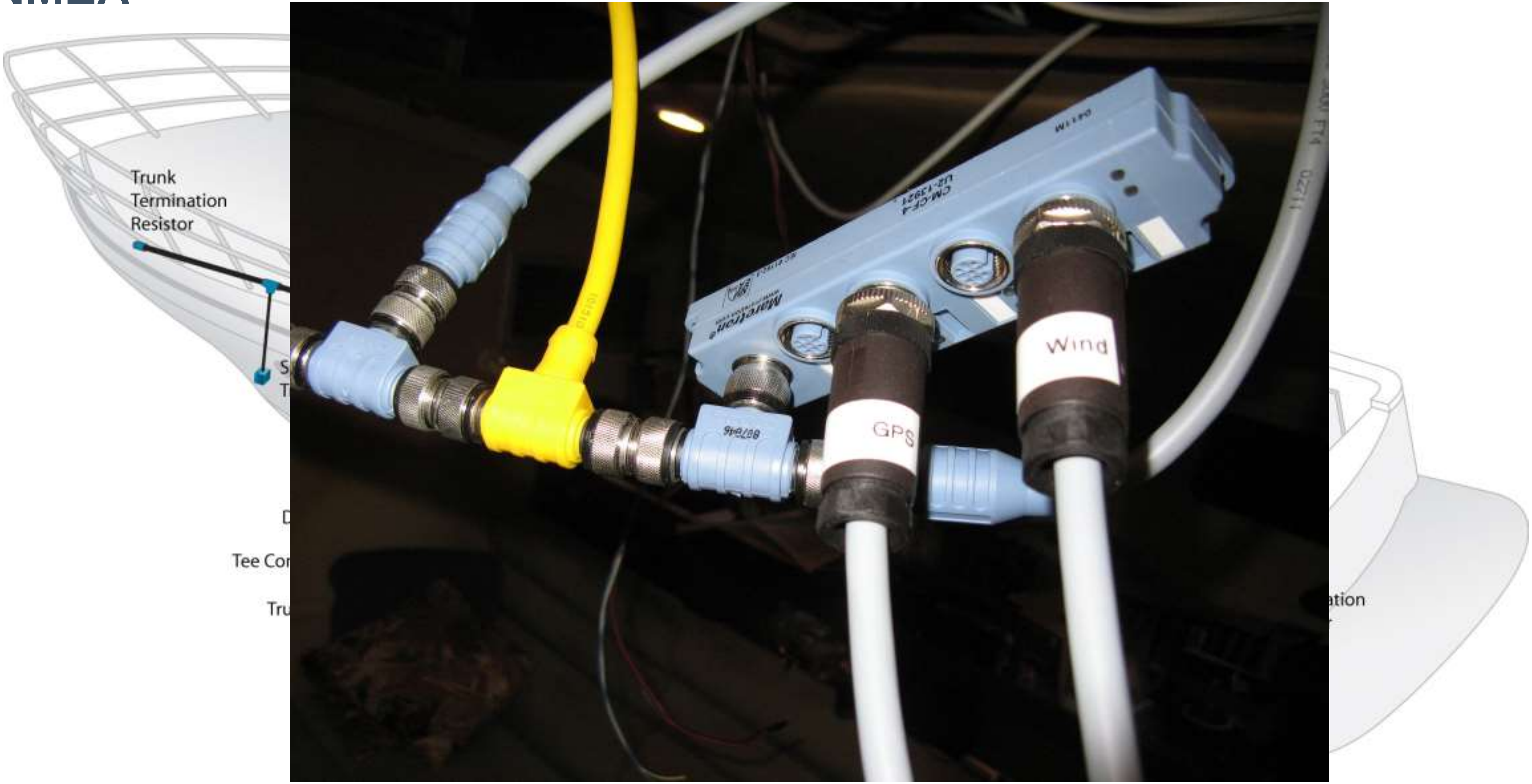
NMEA 2000

bandwidth capacities of less than 1Mbit/s

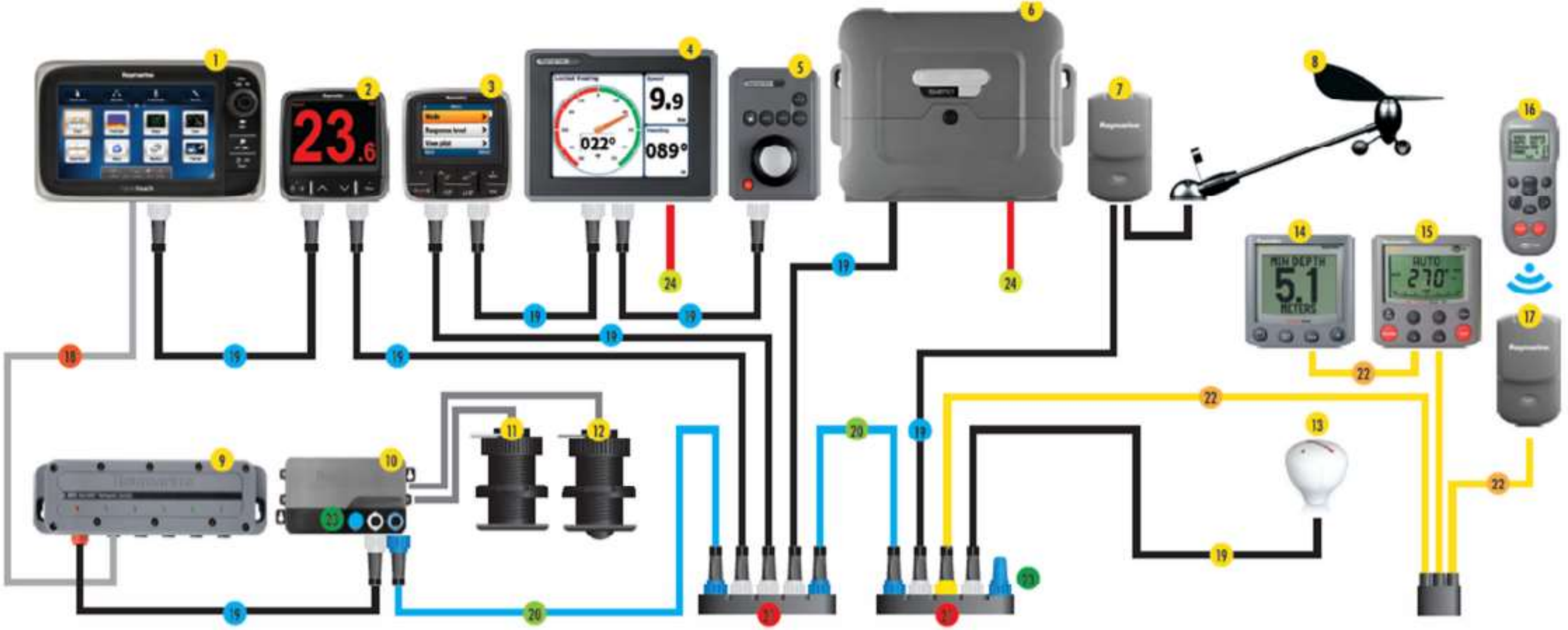
connects devices using Controller Area Network (CAN) technology originally developed for the auto industry.

NMEA 2000 network is not electrically compatible with an NMEA 0183 network

# NMEA


Trunk Termination Resistor
S
T
D
Tee Co
Tru
ation
Maretron
CM-CF-4
U2-13921
GPS
Wind

# SeaTalk$^{ng}$



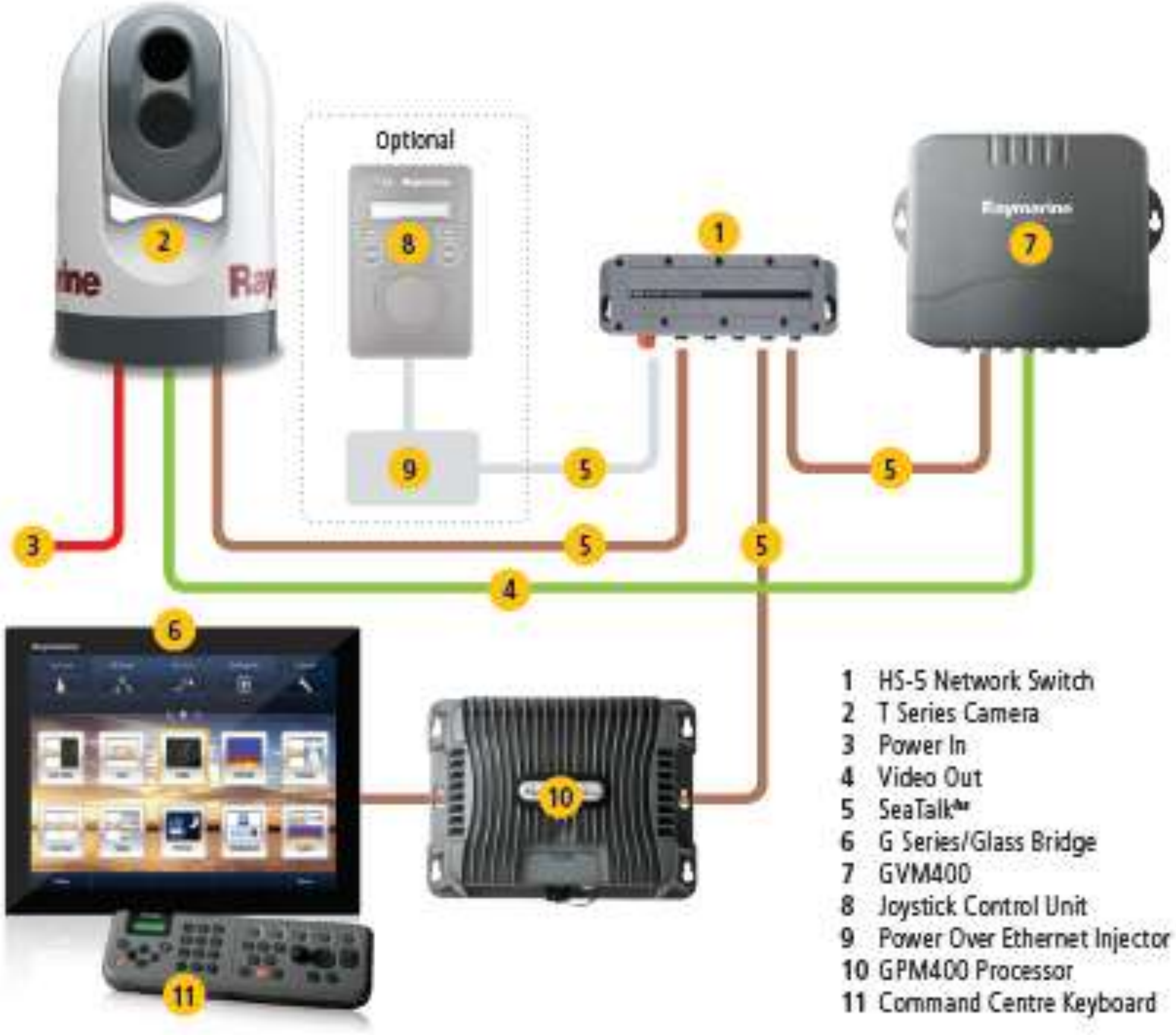
**Note:** Imagery for illustrative purposes only. Product images shown in suggested system diagrams are not to scale

**Typical Basic SeaTalk$^{ng}$ System:**

**1.** New e Series **2.** i70 Instrument **3.** p70/p70R Autopilot **4.** ST70 Plus Instrument **5.** ST70 Plus Autopilot Keypad **6.** SPX Course Computer **7.** Pod **8.** Wind Transducer **9.** Network Switch **10.** iTC-5 **11.** Speed Transducer **12.** Depth Transducer **13.** RS130 GPS Sensor **14.** ST60+ Instrument **15.** ST6002 Autopilot **16.** SmartController **17.** Pod **18.** RayNet Cable **19.** SeaTalk$^{ng}$ Spur **20.** SeaTalk$^{ng}$ Backbone **21.** 5-Way SeaTalk$^{ng}$ Connector **22.** SeaTalk **23.** Terminator **24.** Power Supply

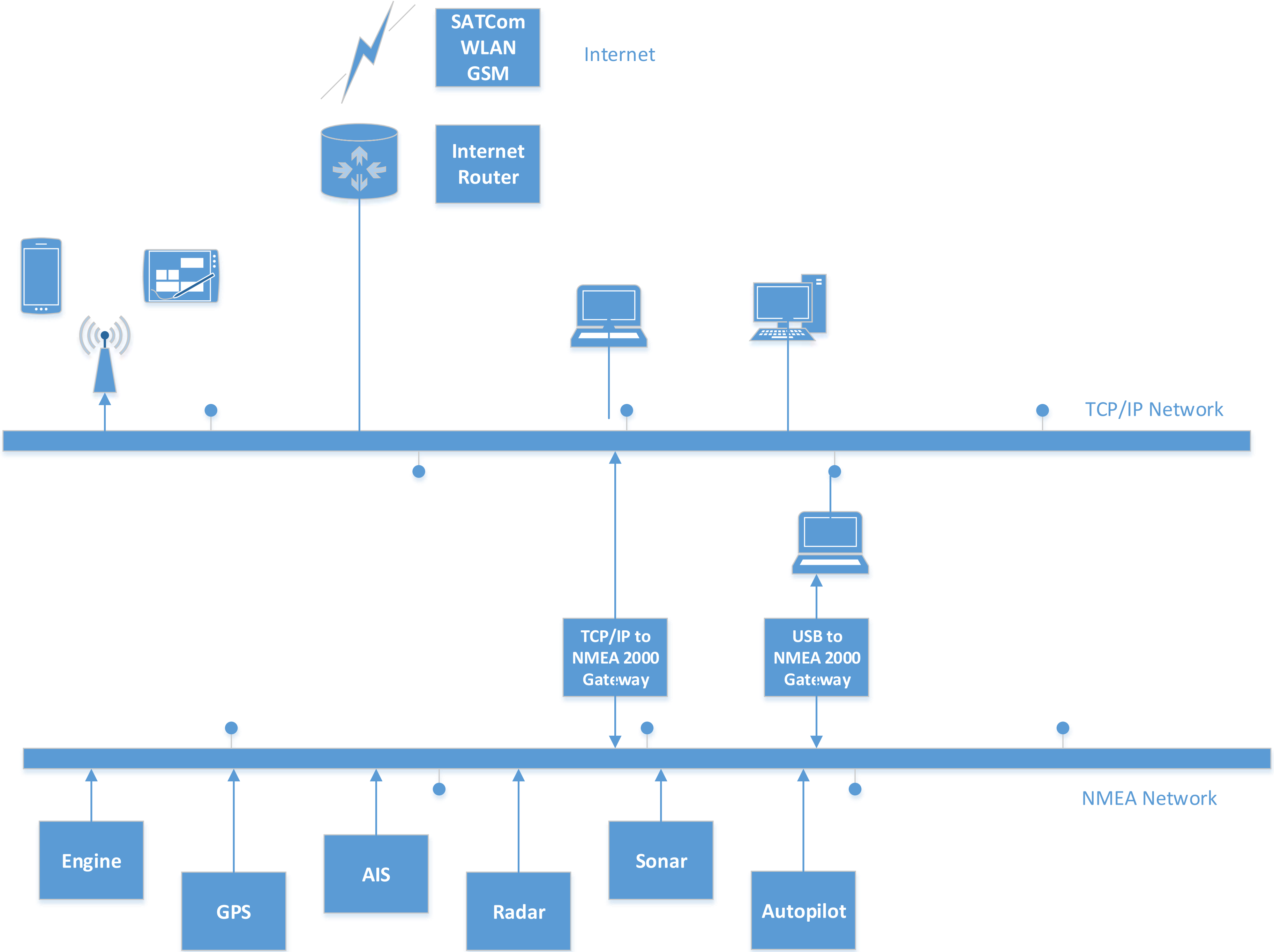
http://www.raymarine.de/uploadedFiles/Products/Networking/SeaTalk/SeaTalkng.pdf

# SeaTalk$^{hs}$



http://www.raymarine.de/uploadedImages/Products/Networking/HS%20with%20HS5%20switch.jpg

# Network


SATCom
WLAN
GSM
Internet
Internet Router
TCP/IP Network
TCP/IP to NMEA 2000 Gateway
USB to NMEA 2000 Gateway
NMEA Network
Engine
GPS
AIS
Radar
Sonar
Autopilot

# Marine Electronic

Vessel Traffic Service (VTS)

Automatic identification system (AIS)

Electronic Chart Display and Information System (ECDIS)

Autopilot

Internet Access

# Vessel traffic service

A vessel traffic service (VTS) is a marine traffic monitoring system established by harbour or port authorities, similar to air traffic control for aircraft.

VTS systems use

- Radar
- closed-circuit television (CCTV)
- VHF radiotelephony
- automatic identification system

# Automatic identification system (AIS)

AIS is an automatic tracking system used

- on ships and
- by vessel traffic services (VTS).

*Satellite-AIS* (S-AIS)

- satellites are used to detect AIS signatures

# Automatic identification system (AIS)

AIS information supplements marine radar,

- similar to GPS in Aircrafts –

which continues to be the primary method of collision avoidance for water transport.

# Electronic Chart Display and Information System (ECDIS)

ECDIS is a geographic information system used for nautical navigation

displays information from:

- Electronic Navigational Charts (ENC)
- or Digital Nautical Charts (DNC)

mud, clay
Entrance Point Light 127
mud, clay

integrates position information

- Position
- Heading
- speed

sensors which could interface with an ECDIS are radar, Navtex, Automatic Identification Systems (AIS), and depth sounders.

# IT Equipment on Board

Internet Access

- GSM
- WiFi
- SAT (Inmarsat, VSAT, Iridium, etc. )

On Board

- Entertainment Systems
- WiFi (Crew, Guest/Owner)
- VoIP

# IT equipment on Board

10 Smart TV & Sat Receiver

1 Chart PC

14 VoIP Telephones

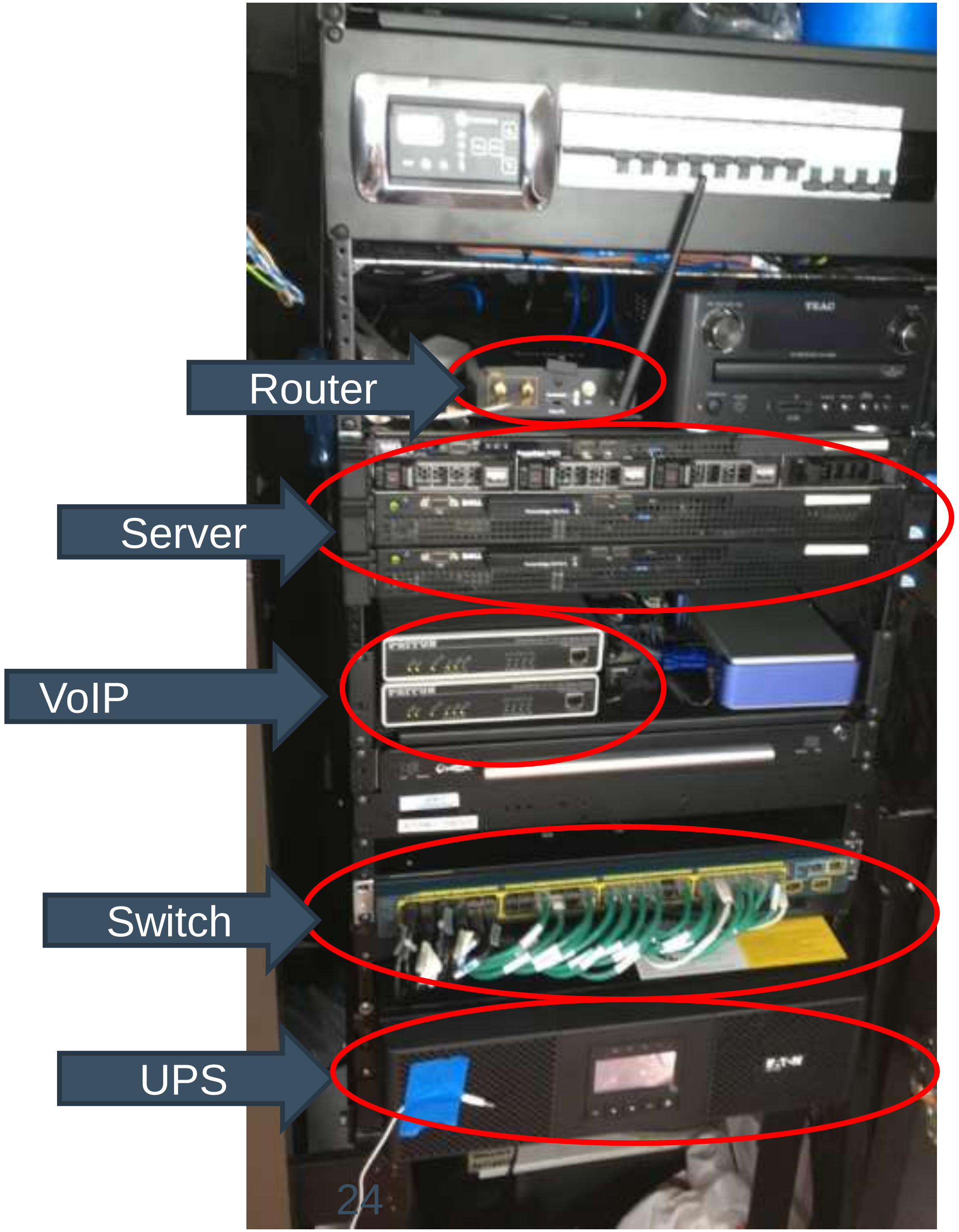
1 Internet Router (GSM, WiFi, SAT)

1 rack mounted Switch (48ports)

1 UPS

4 WiFi Access Point

(Crew, Guest/Owner)



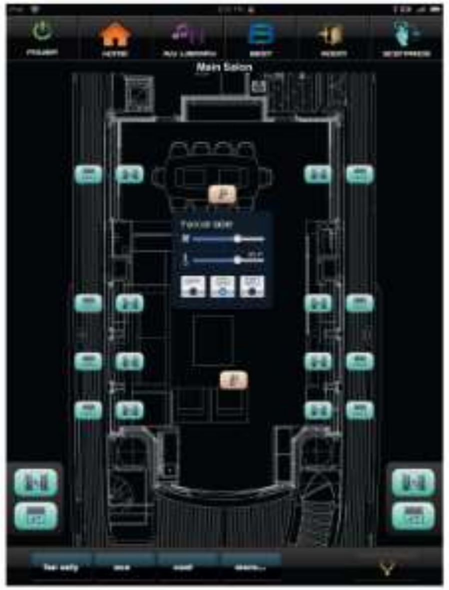
# Smart Ships

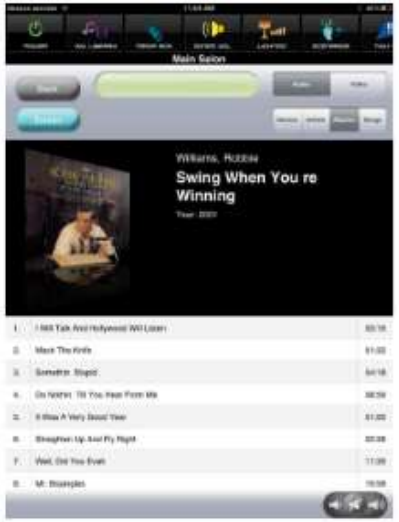
Audio & Video Streaming

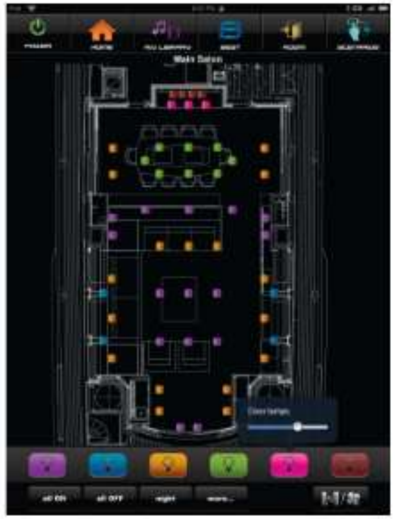
iPhone/iPad remote control of

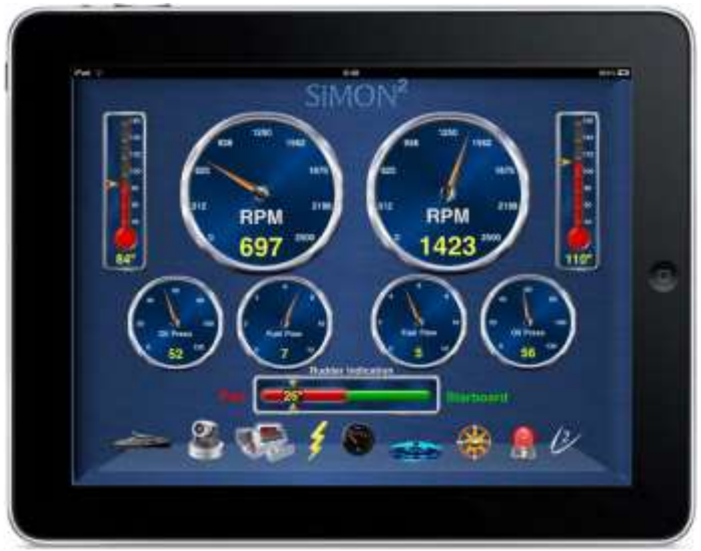
- Lights
- Electric curtains
- Engine monitor

Etc.

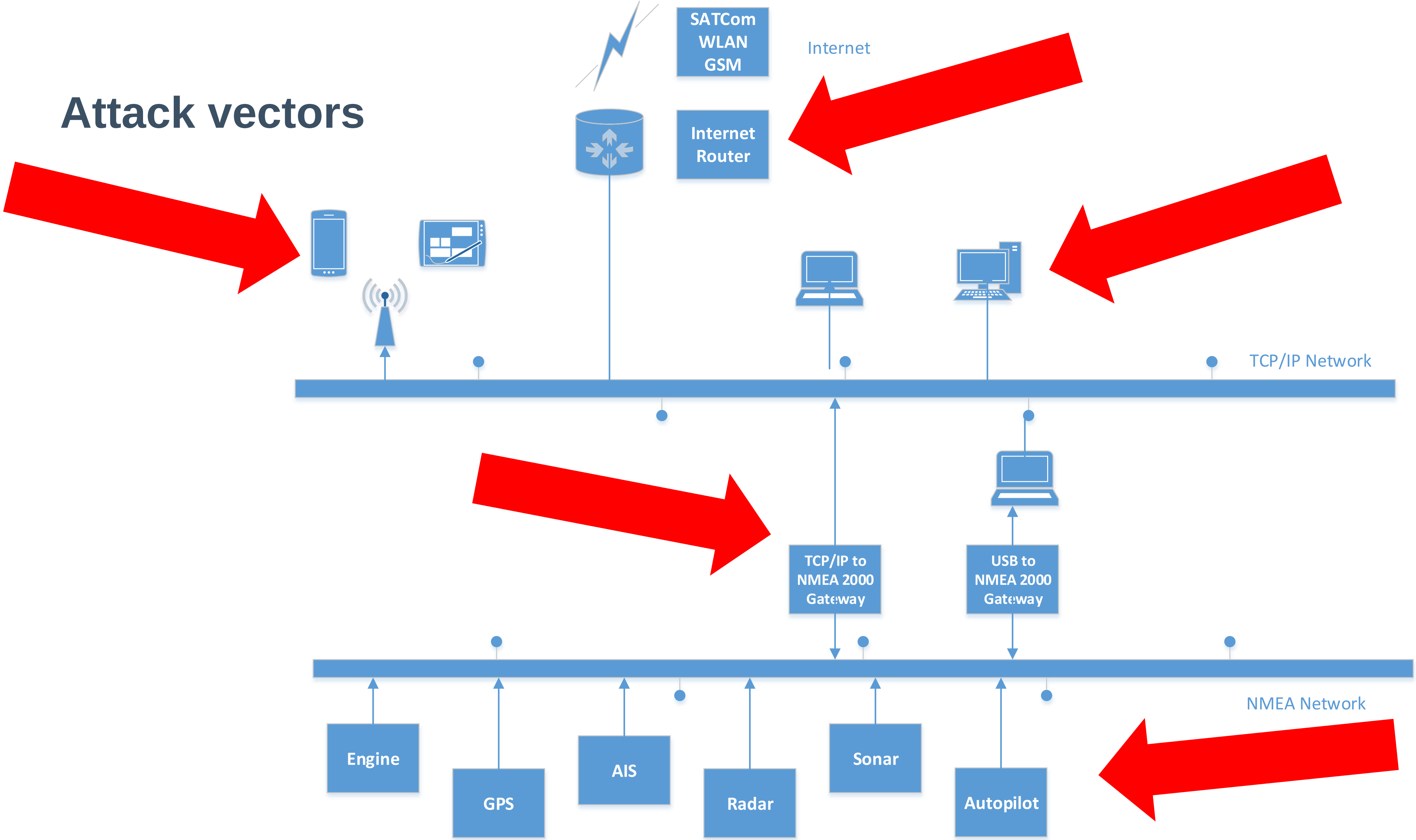








# Attack vectors



# Attack vectors

- GPS
- AIS
- Autopilot
- IT equipment on Board
- Internet connection routers (VSAT, InmarSat, GSM, WLAN, etc.)
- Cloud based services

**GPS**

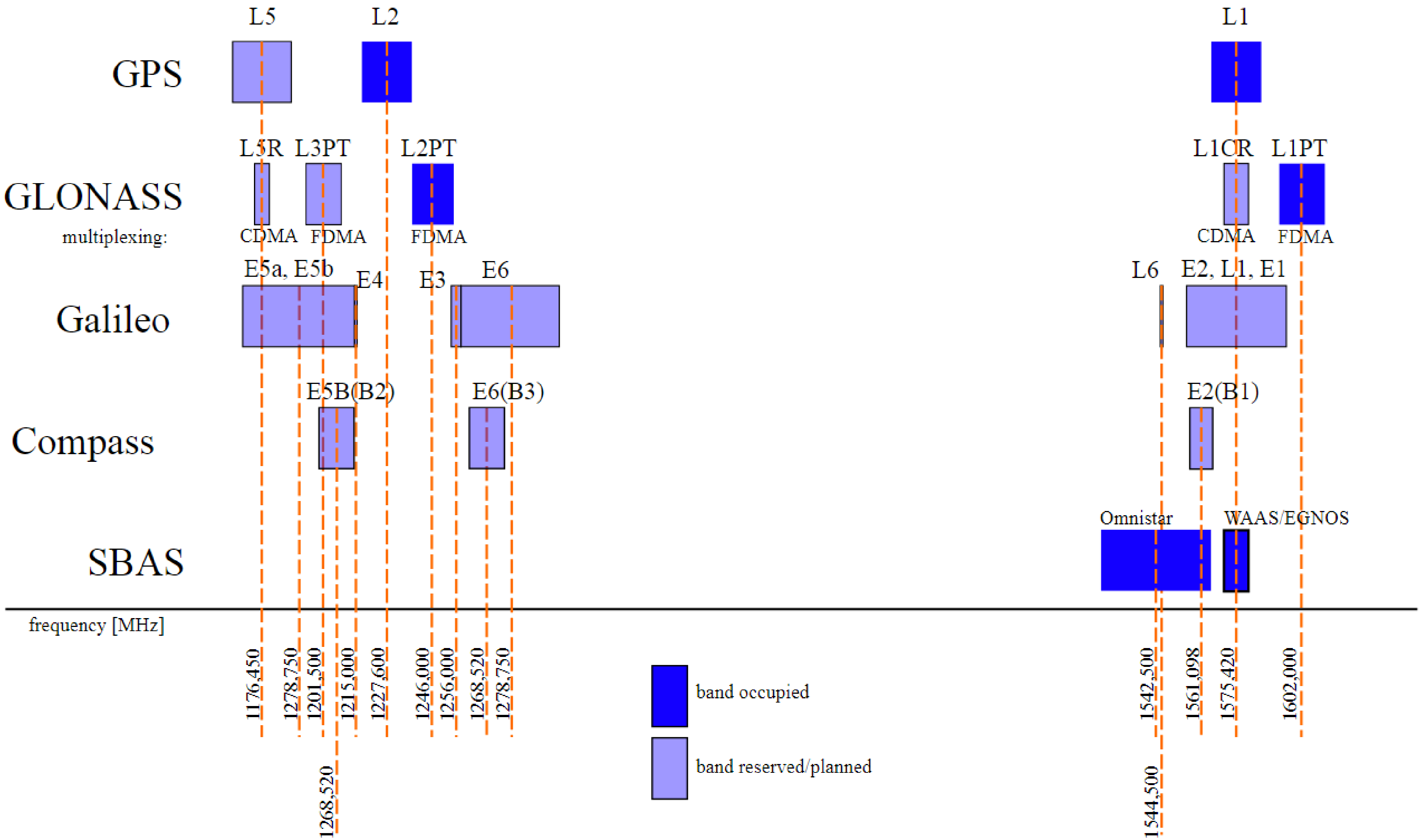
# GNSS or GPS attacks

# GPS – many different systems

GNSS (global Navigation satellite system)

- NAVSTAR GPS (United Staates of America)
- GLONASS (Russian Föderation)
- Galileo (Europe Union)
- Beidou (China)

# GPS – many different systems



https://upload.wikimedia.org/wikipedia/commons/9/9a/Gnss_bandwidth.svg

# GPS

2 Scenarios are possible

- jamming
- spoofing

complexibility:

Jamming = quite simple

Spoofing = complex – feasible for under1000 Euro

# GPS attacks

Spoofing GPS signal is not that easy

Minimum 3 different Satellite signal has to be spoofed

Commercial ships and bigger yachts have backup GPS (Navstar + Galileo)

Some GPS receiver can detect position jumps

It’s easier to fake the NMEA data of the GPS Sensor

# GPS - Jamming

Eastern Pacific reports more and more GPS anomalies

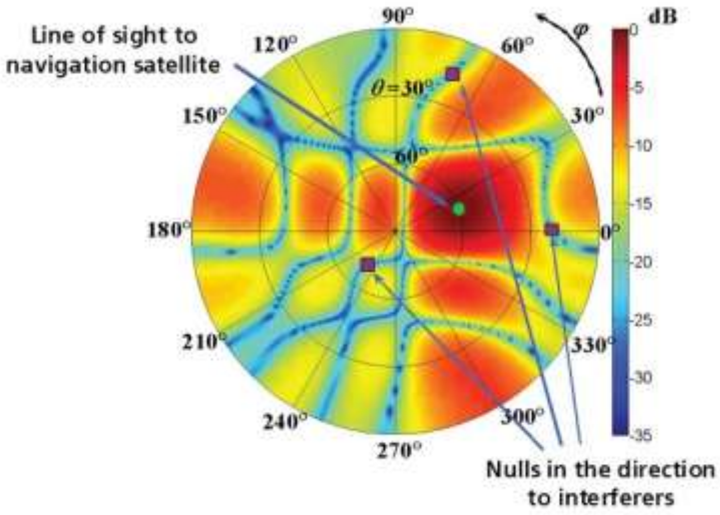
- Juni, week 25 – more than 20 reports – north east black see
- NATO Troops maneuver at same time there
- Sept. Norway reports anomalies in a height >2000ft
- https://rntfnd.org/wp-content/uploads/Norway-Comms-Auth-Report-GPS-Jamming-Sept-2017.pdf

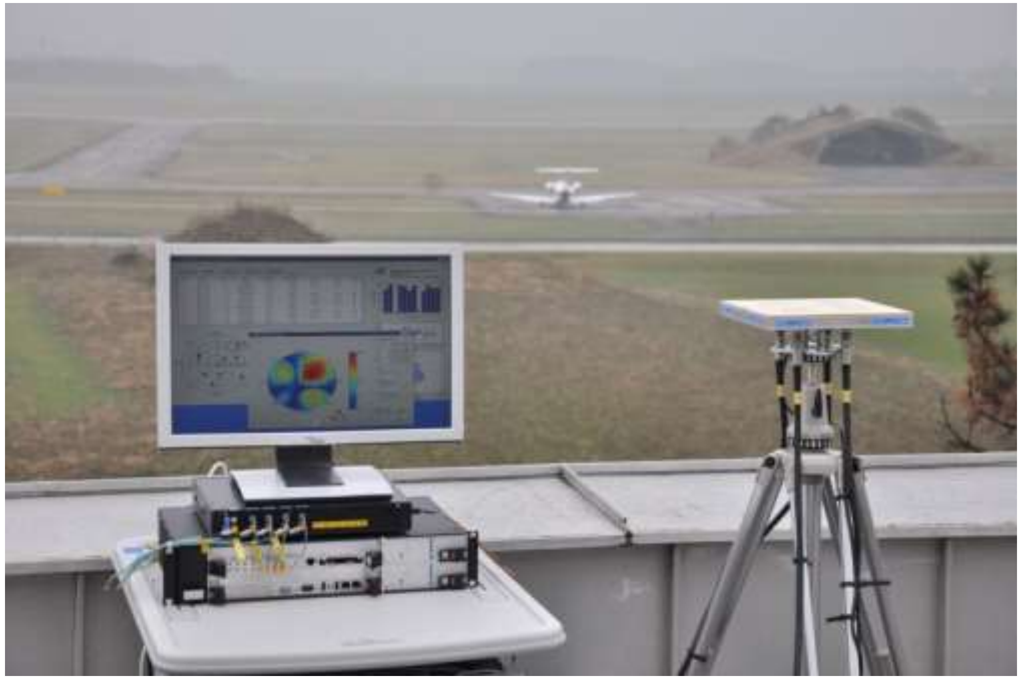
- US Navy teaching again offline Navigation with Sixtant

# Securing GPS?

Research Project – „Galant“ by DLR – Institute of communications and navigation

- 2x2 active antenna array
- Beamforming & array processing





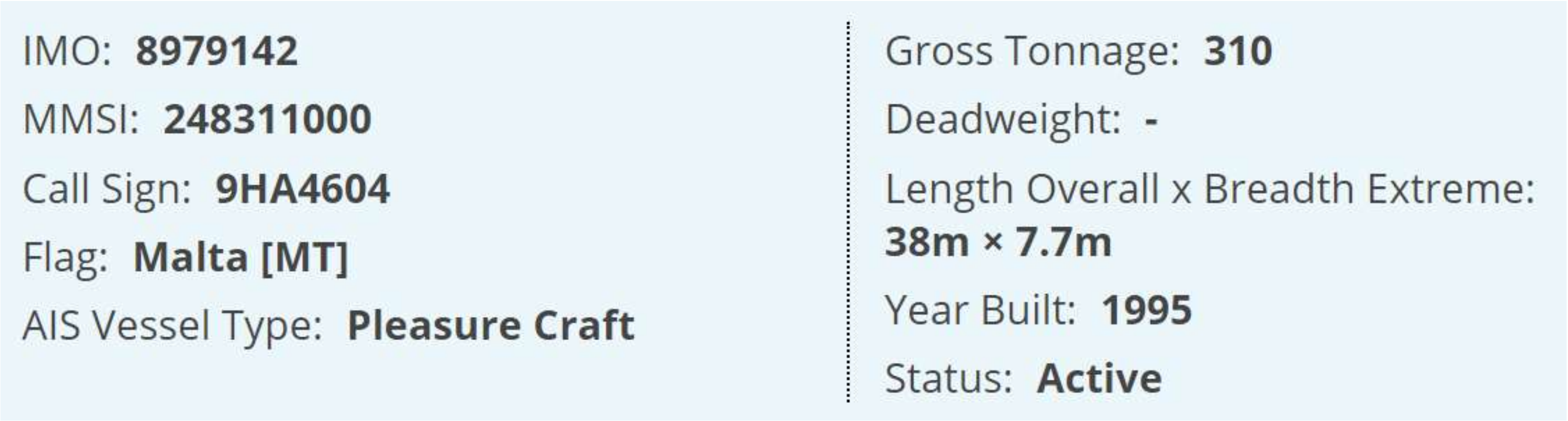
http://www.dlr.de/kn/en/desktopdefault.aspx/tabid-4306/6938_read-9224/

# Automatic identification system (#1)

Following Data a AIS transceiver sends every 2 to 10 seconds while underway,
and every 3 minutes while a vessel is at anchor:

- Maritime Mobile Service Identity (MMSI) – a unique nine digit identification number.
- Navigation status – "at anchor", "under way using engine(s)", "not under command", etc.
- Rate of turn – right or left, from 0 to 720 degrees per minute
- Speed over ground – 0.1-knot (0.19 km/h) resolution from 0 to 102 knots (189 km/h)
- Positional accuracy: Longitude & Latitude – to 0.0001 minutes
- Course over ground – relative to true north to 0.1°
- True heading – 0 to 359 degrees (for example from a gyro compass)
- True bearing at own position. 0 to 359 degrees
- UTC Seconds

# Automatic identification system



IMO: **8979142**

MMSI: **248311000**

Call Sign: **9HA4604**

Flag: **Malta [MT]**

AIS Vessel Type: **Pleasure Craft**

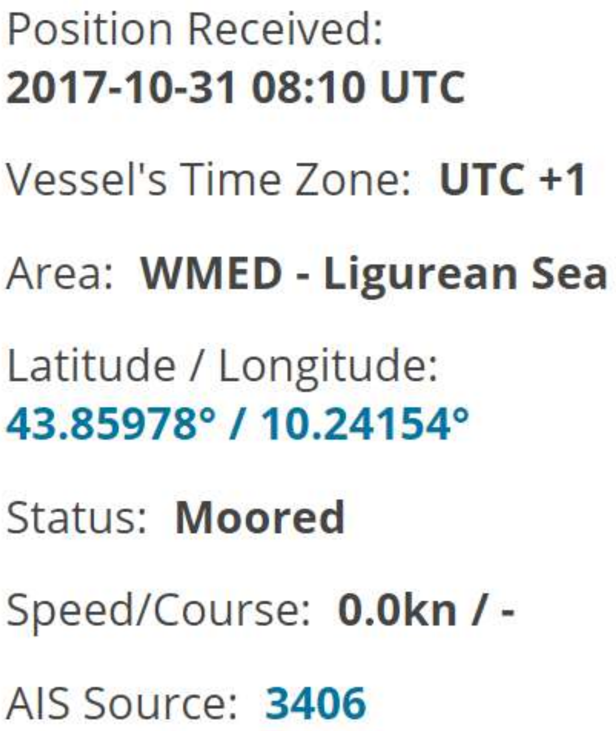
Gross Tonnage: **310**

Deadweight: **-**

Length Overall x Breadth Extreme: **38m × 7.7m**

Year Built: **1995**

Status: **Active**



Position Received: **2017-10-31 08:10 UTC**

Vessel's Time Zone: **UTC +1**

Area: **WMED - Ligurean Sea**

Latitude / Longitude: **43.85978° / 10.24154°**

Status: **Moored**

Speed/Course: **0.0kn / -**

AIS Source: **3406**

# Automatic identification system (#1)

Following Data a AIS transceiver sends every 2 to 10 seconds while underway,
and every 3 minutes while a vessel is at anchor:

- Maritime Mobile Service Identity (MMSI) – a unique nine digit identification number.
- Navigation status – "at anchor", "under way using engine(s)", "not under command", etc.
- Rate of turn – right or left, from 0 to 720 degrees per minute
- Speed over ground – 0.1-knot (0.19 km/h) resolution from 0 to 102 knots (189 km/h)
- Positional accuracy: Longitude & Latitude – to 0.0001 minutes
- Course over ground – relative to true north to 0.1°
- True heading – 0 to 359 degrees (for example from a gyro compass)
- True bearing at own position. 0 to 359 degrees
- UTC Seconds

# Automatic identification system (#2)

following data are broadcast every 6 minutes:

- IMO ship identification number – a seven digit number that remains unchanged
- Radio call sign – international radio call sign,
- Name – 20 characters to represent the name of the vessel
- Type of ship/cargo
- Dimensions of ship – to nearest meter
- Location of positioning system's (e.g., GPS) antenna on board the vessel - in meters aft of bow and meters port or starboard
- Type of positioning system – such as GPS, DGPS or LORAN-C.
- Draught of ship – 0.1 meter to 25.5 meters
- Destination – max. 20 characters
- ETA (estimated time of arrival) at destination – UTC month/date hour:minute

optional : high precision time request, a vessel can request other vessels provide a high precision UTC time and datestamp

## AIS RF part

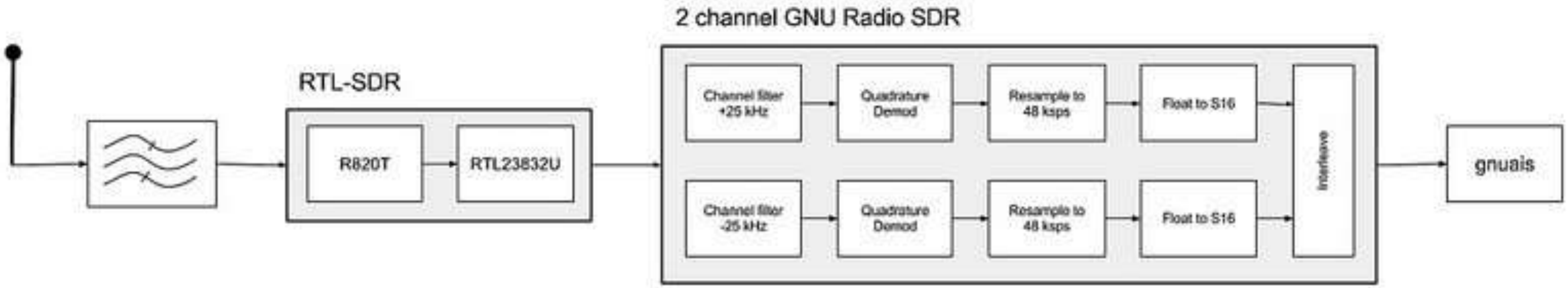
AIS uses the globally allocated Marine Band channels 87 & 88.

AIS uses the high side of the duplex from VHF radio "channels" (87B) & (88B)

- Channel A 161.975 MHz (87B)
- Channel B 162.025 MHz (88B)
- Before being transmitted, AIS messages must be NRZI encoded.
- AIS messages are GMSK modulated.
- transmission bit rate is 9600bit/s

# AIS hacking

2-CHANNEL AIS RECEIVER WITH RTL-SDR AND GNUAIS



https://www.rtl-sdr.com/2-channel-ais-receiver-rtl-sdr-gnuais/

# Autopilot (future Project – started already)

Remote control for heading & speed !

No issues found yet

I am working on it !

# Autopilot

Raymarine S100 wireless Remote Control

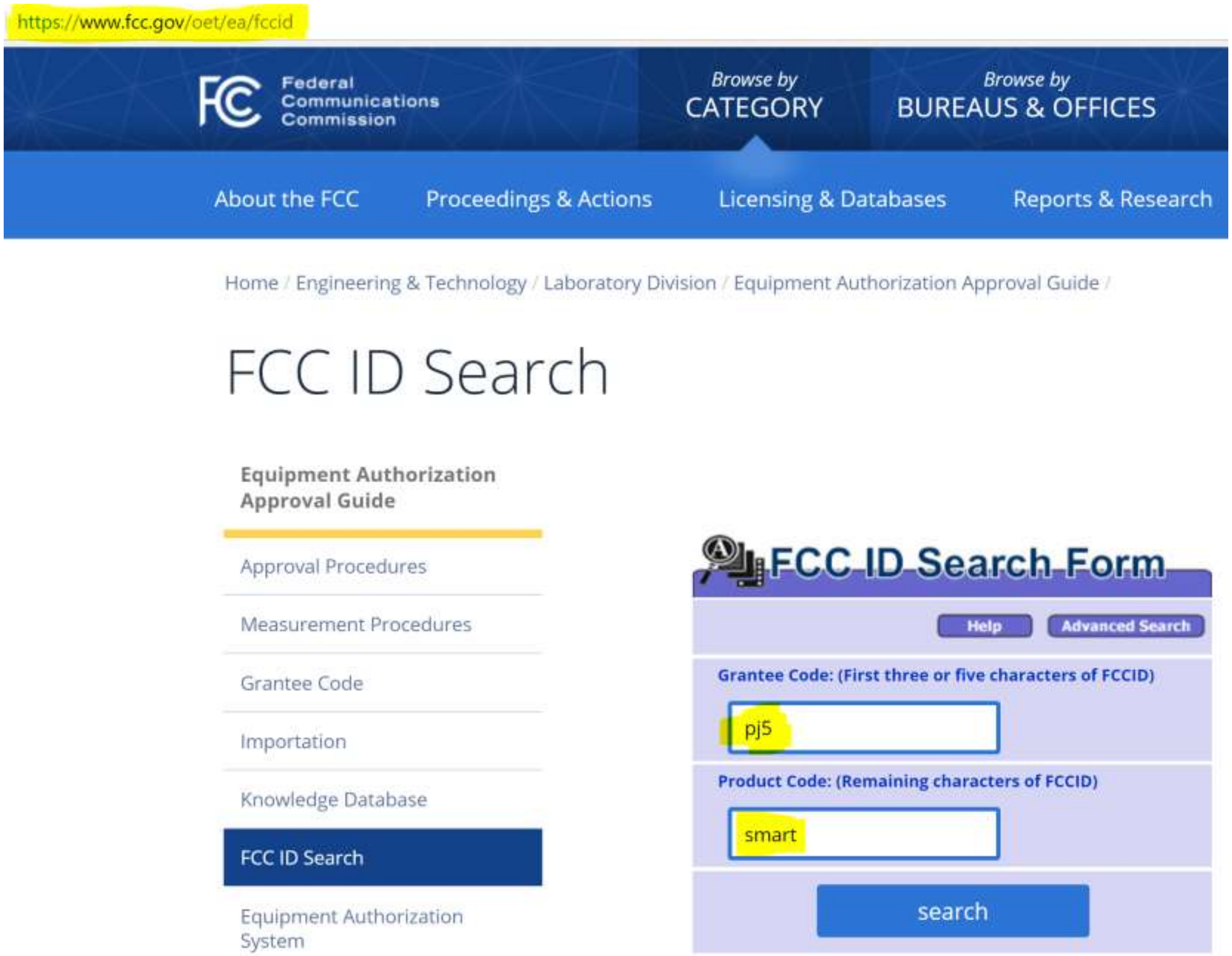
The compact Raymarine S100 remote control gives you basic, onboard wireless control of any Raymarine SeaTalk autopilot, even if you're below deck and out of sight of your autopilot.

## Key Features

- Two lines of text
- Signal strength indicator
- Out of range of base station warning

# Autopilot

FCC ID search



https://www.fcc.gov/oet/ea/fccid

Home / Engineering & Technology / Laboratory Division / Equipment Authorization Approval Guide /

## FCC ID Search

FCC ID Search Form

Grantee Code: (First three or five characters of FCCID)

pj5

Product Code: (Remaining characters of FCCID)

smart

# Autopilot

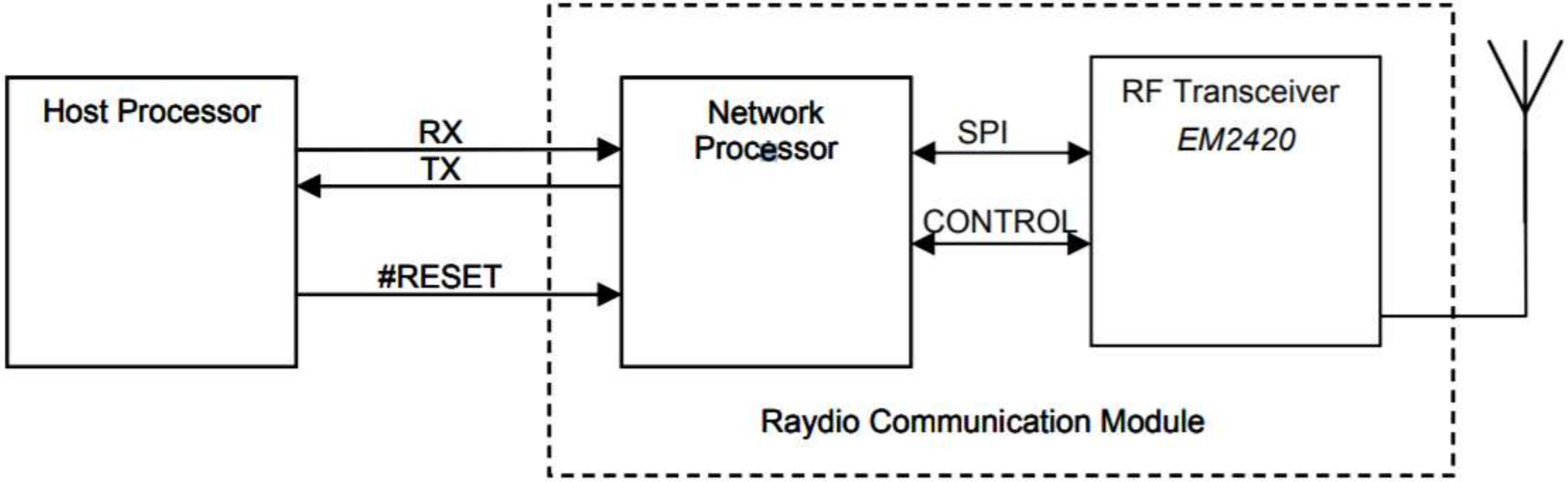
Raymarine Autopilot S100 Handheld

- FCC ID PJ5Smart
- Communicates with the S1000 Autopilot
- Operates wireless on 2.45GHz
- Is not WiFi

## Autopilot

RCM is based upon Ember’s EM2420 2.45GHz RF transceiver connected to an ATMEGA64 microprocessor

runs on Emberstack



FANDANGO
MOVIECLIPS

## Yacht Router hacking

Locomarine

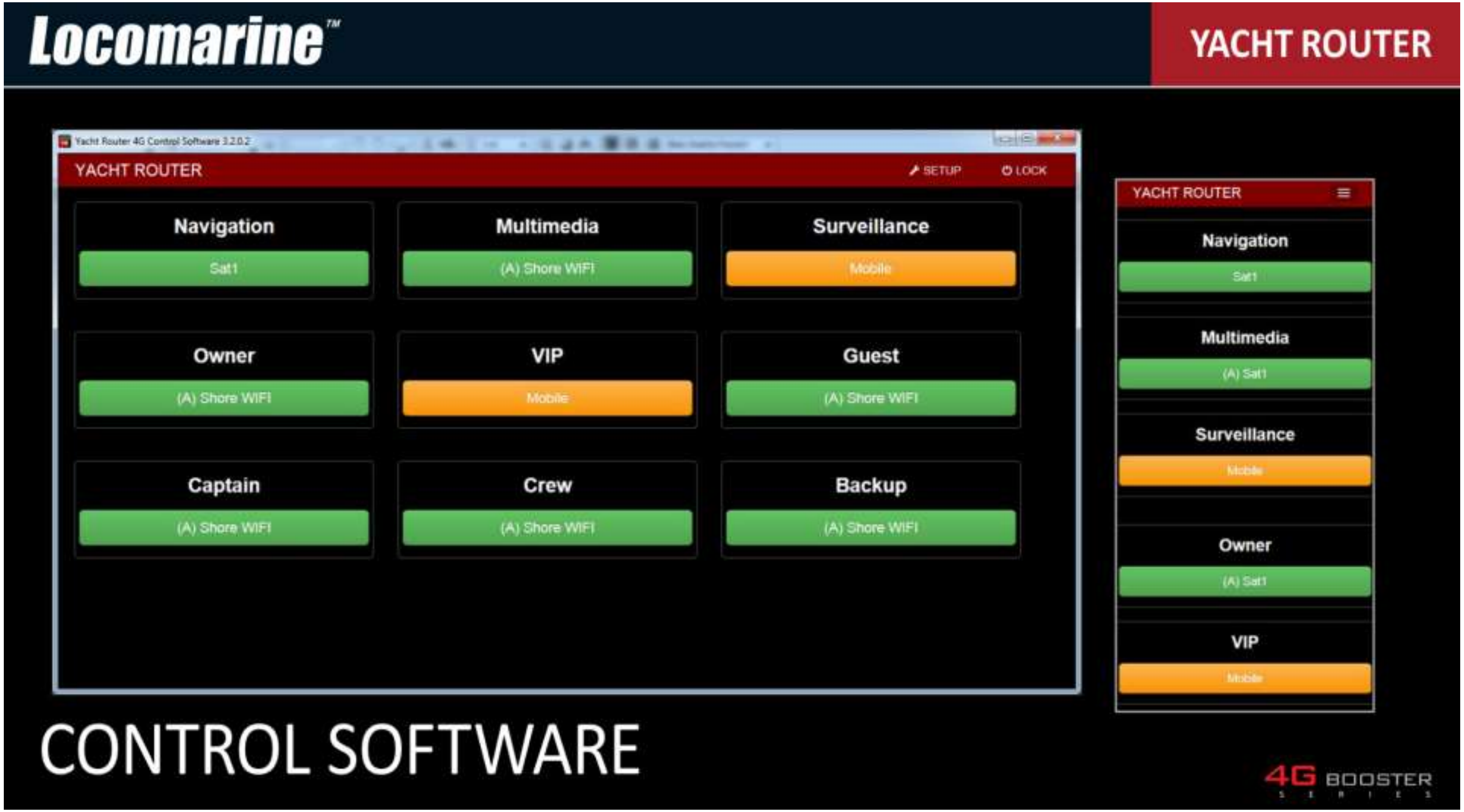
Yachtrouter

# Yacht Router hacking

Locomarine Yachtrouter

- High power WIFI Booster for long distance connectivity (15+ NM)
- High power 4G/3G/2G module (30+ Nautical miles)

# Issue #1 – The control software



Locomarine™

YACHT ROUTER

Yacht Router 4G Control Software 3.2.0.2

YACHT ROUTER SETUP LOCK

| | | |
|---|---|---|
| Navigation<br>Sat1 | Multimedia<br>(A) Shore WIFI | Surveillance<br>Mobile |
| Owner<br>(A) Shore WIFI | VIP<br>Mobile | Guest<br>(A) Shore WIFI |
| Captain<br>(A) Shore WIFI | Crew<br>(A) Shore WIFI | Backup<br>(A) Shore WIFI |

YACHT ROUTER

Navigation
Sat1

Multimedia
(A) Sat1

Surveillance
Mobile

Owner
(A) Sat1

VIP
Mobile

CONTROL SOFTWARE

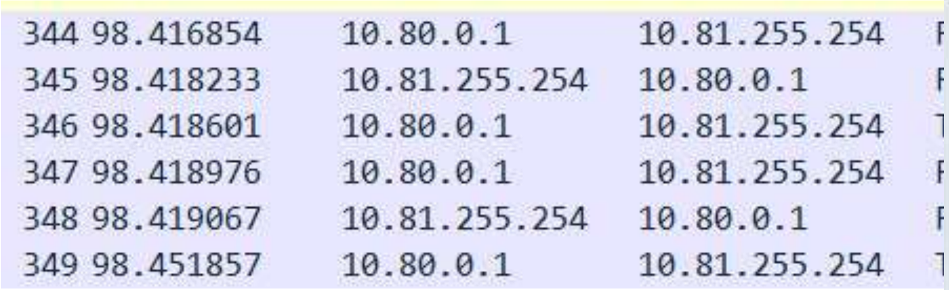
4G BOOSTER SERIES

# Issue #1 – The control software

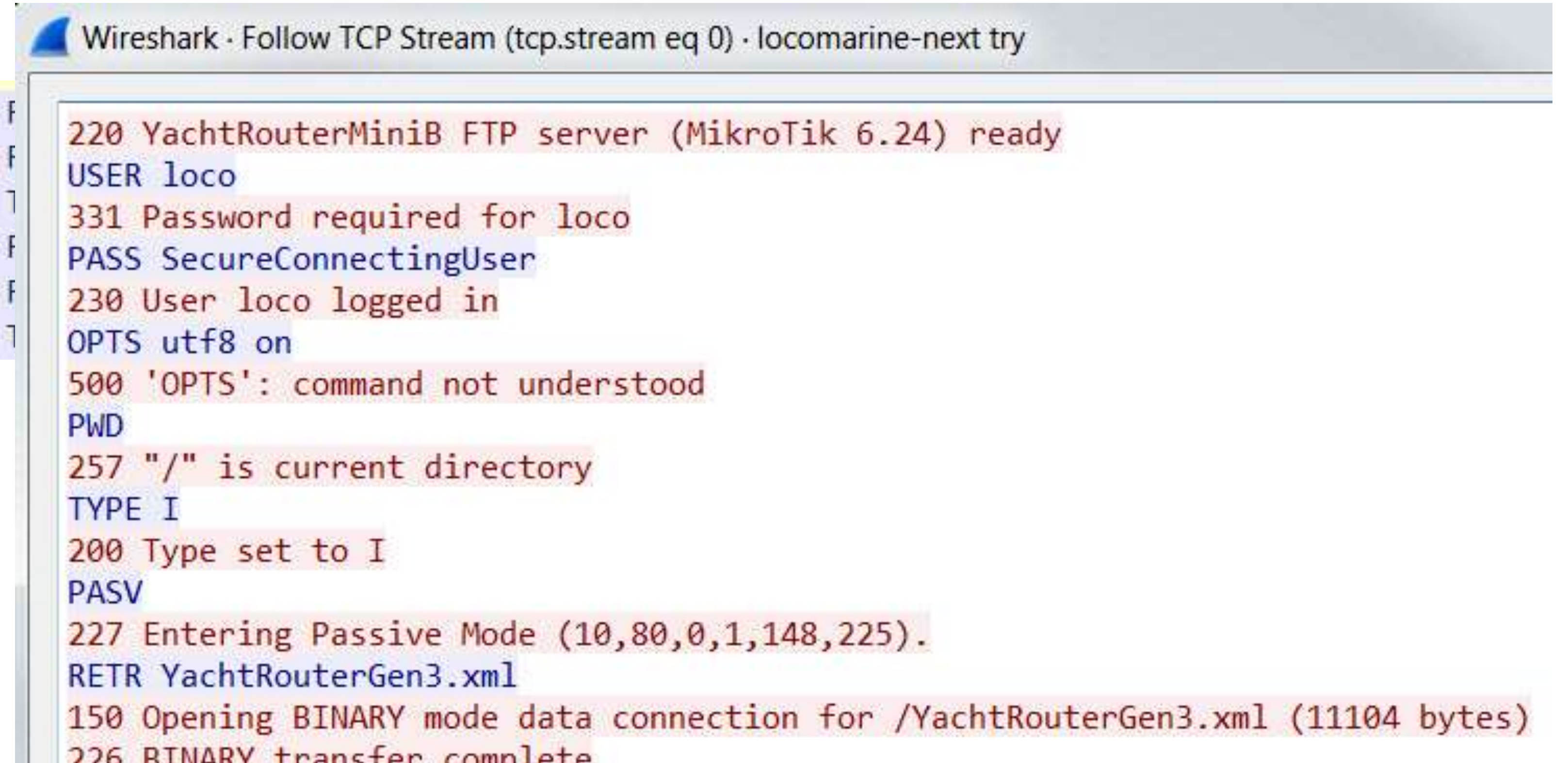
- FTP connect to router
- Download “YachtRouterGen3.xml
- The APP changes settings in the XML
- Uploaded to the Router

# Issue #1 – The control software

- FTP is clear text
- Hardcoded credentials used !!!
- …xml file contains WLAN SSID and Password (clear text)



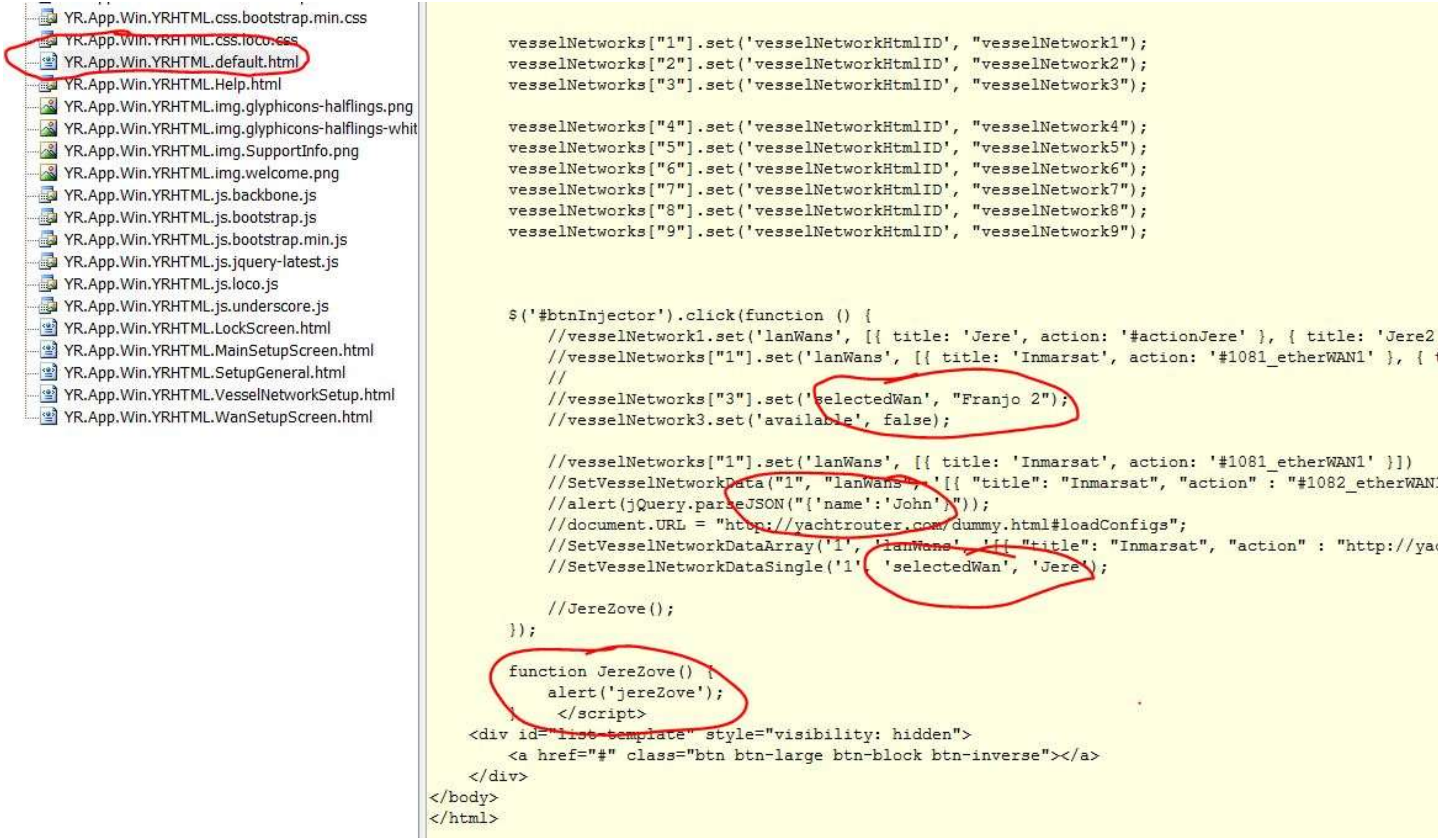
```
344 98.416854    10.80.0.1       10.81.255.254   F
345 98.418233    10.81.255.254   10.80.0.1       F
346 98.418601    10.80.0.1       10.81.255.254   T
347 98.418976    10.80.0.1       10.81.255.254   F
348 98.419067    10.81.255.254   10.80.0.1       F
349 98.451857    10.80.0.1       10.81.255.254   T
```



Wireshark · Follow TCP Stream (tcp.stream eq 0) · locomarine-next try

```
220 YachtRouterMiniB FTP server (MikroTik 6.24) ready
USER loco
331 Password required for loco
PASS SecureConnectingUser
230 User loco logged in
OPTS utf8 on
500 'OPTS': command not understood
PWD
257 "/" is current directory
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (10,80,0,1,148,225).
RETR YachtRouterGen3.xml
150 Opening BINARY mode data connection for /YachtRouterGen3.xml (11104 bytes)
226 BINARY transfer complete
```

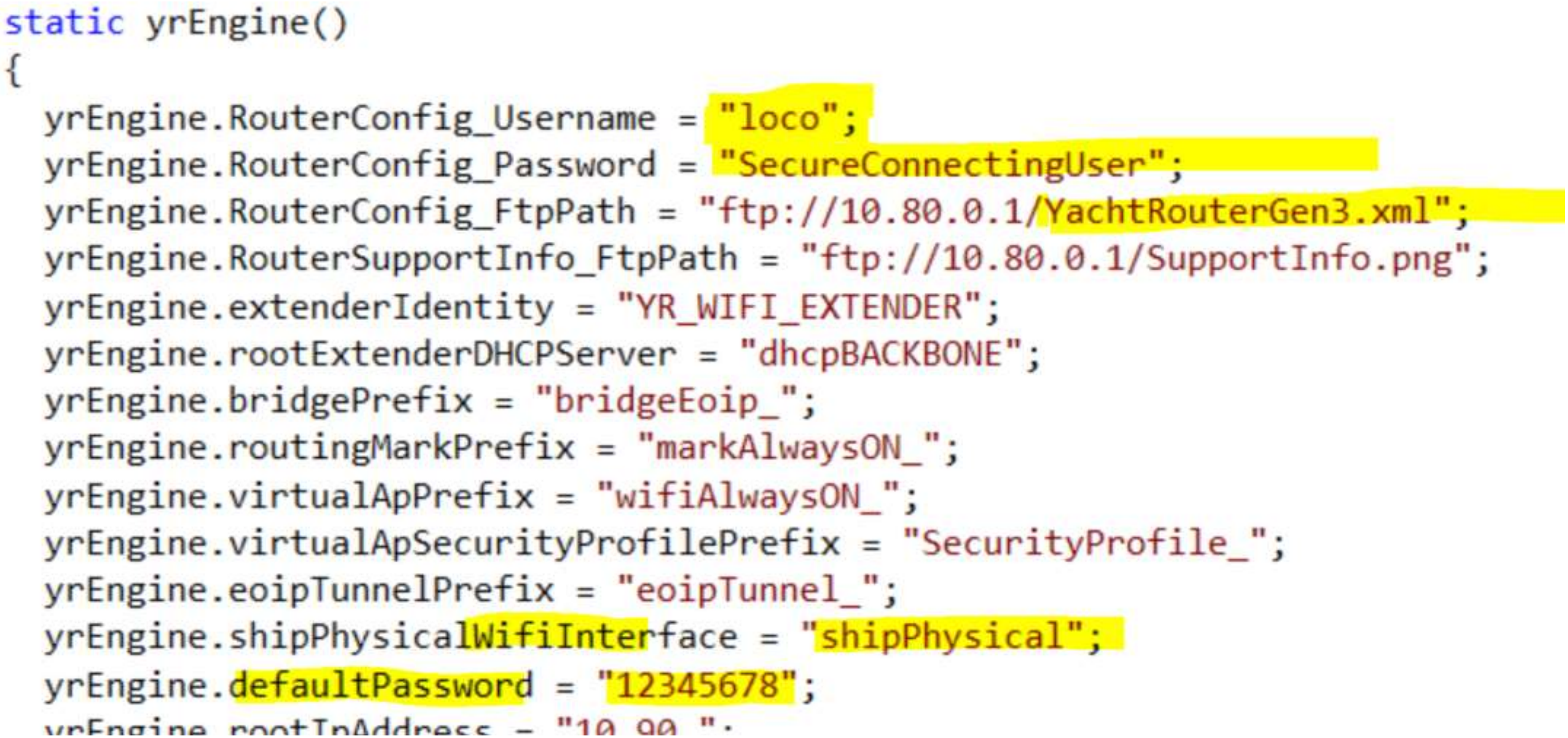
# Issue #2 – code contains juicy informations



```
YR.App.Win.YRHTML.css.bootstrap.min.css
YR.App.Win.YRHTML.css.loco.css
YR.App.Win.YRHTML.default.html
YR.App.Win.YRHTML.Help.html
YR.App.Win.YRHTML.img.glyphicons-halflings.png
YR.App.Win.YRHTML.img.glyphicons-halflings-whit
YR.App.Win.YRHTML.img.SupportInfo.png
YR.App.Win.YRHTML.img.welcome.png
YR.App.Win.YRHTML.js.backbone.js
YR.App.Win.YRHTML.js.bootstrap.js
YR.App.Win.YRHTML.js.bootstrap.min.js
YR.App.Win.YRHTML.js.jquery-latest.js
YR.App.Win.YRHTML.js.loco.js
YR.App.Win.YRHTML.js.underscore.js
YR.App.Win.YRHTML.LockScreen.html
YR.App.Win.YRHTML.MainSetupScreen.html
YR.App.Win.YRHTML.SetupGeneral.html
YR.App.Win.YRHTML.VesselNetworkSetup.html
YR.App.Win.YRHTML.WanSetupScreen.html
```

```
        vesselNetworks["1"].set('vesselNetworkHtmlID', "vesselNetwork1");
        vesselNetworks["2"].set('vesselNetworkHtmlID', "vesselNetwork2");
        vesselNetworks["3"].set('vesselNetworkHtmlID', "vesselNetwork3");

        vesselNetworks["4"].set('vesselNetworkHtmlID', "vesselNetwork4");
        vesselNetworks["5"].set('vesselNetworkHtmlID', "vesselNetwork5");
        vesselNetworks["6"].set('vesselNetworkHtmlID', "vesselNetwork6");
        vesselNetworks["7"].set('vesselNetworkHtmlID', "vesselNetwork7");
        vesselNetworks["8"].set('vesselNetworkHtmlID', "vesselNetwork8");
        vesselNetworks["9"].set('vesselNetworkHtmlID', "vesselNetwork9");



        $('#btnInjector').click(function () {
            //vesselNetwork1.set('lanWans', [{ title: 'Jere', action: '#actionJere' }, { title: 'Jere2
            //vesselNetworks["1"].set('lanWans', [{ title: 'Inmarsat', action: '#1081_etherWAN1' }, {
            //
            //vesselNetworks["3"].set('selectedWan', "Franjo 2");
            //vesselNetwork3.set('available', false);

            //vesselNetworks["1"].set('lanWans', [{ title: 'Inmarsat', action: '#1081_etherWAN1' }])
            //SetVesselNetworkData("1", "lanWans", '[{ "title": "Inmarsat", "action" : "#1082_etherWAN
            //alert(jQuery.parseJSON("{'name':'John'}"));
            //document.URL = "http://yachtrouter.com/dummy.html#loadConfigs";
            //SetVesselNetworkDataArray('1', 'lanWans', '[{ "title": "Inmarsat", "action" : "http://ya
            //SetVesselNetworkDataSingle('1', 'selectedWan', 'Jere');

            //JereZove();
        });

        function JereZove() {
            alert('jereZove');
        }
    </script>
    <div id="list-template" style="visibility: hidden">
        <a href="#" class="btn btn-large btn-block btn-inverse"></a>
    </div>
</body>
</html>
```

# Issue #2 – code contains juicy informations



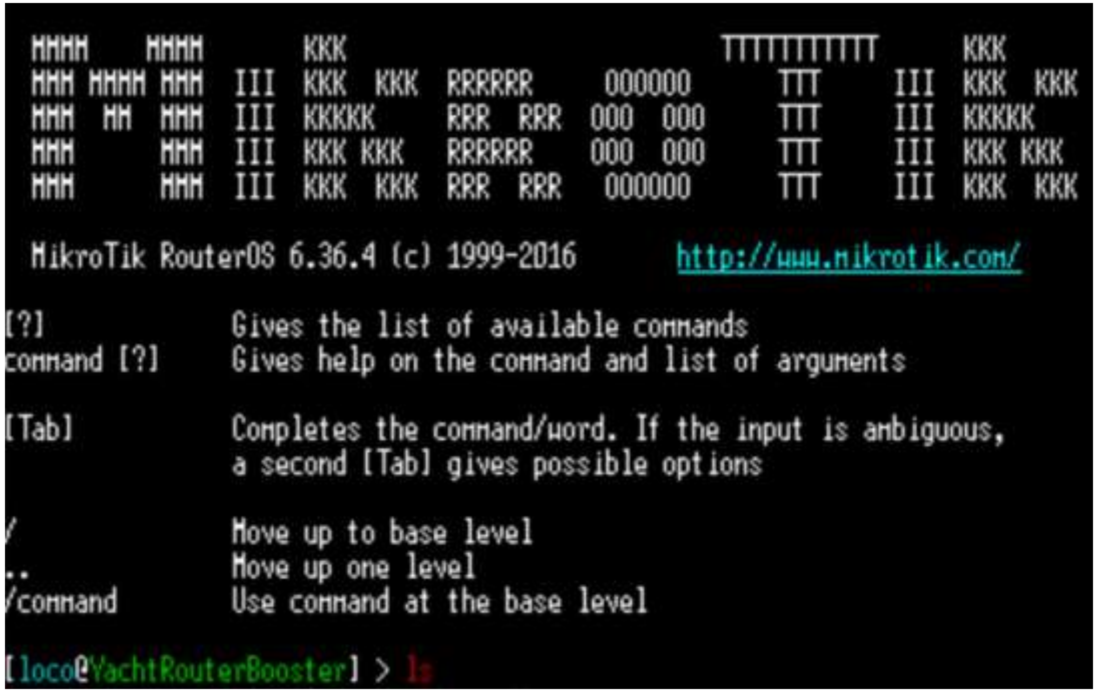
```
static yrEngine()
{
  yrEngine.RouterConfig_Username = "loco";
  yrEngine.RouterConfig_Password = "SecureConnectingUser";
  yrEngine.RouterConfig_FtpPath = "ftp://10.80.0.1/YachtRouterGen3.xml";
  yrEngine.RouterSupportInfo_FtpPath = "ftp://10.80.0.1/SupportInfo.png";
  yrEngine.extenderIdentity = "YR_WIFI_EXTENDER";
  yrEngine.rootExtenderDHCPServer = "dhcpBACKBONE";
  yrEngine.bridgePrefix = "bridgeEoip_";
  yrEngine.routingMarkPrefix = "markAlwaysON_";
  yrEngine.virtualApPrefix = "wifiAlwaysON_";
  yrEngine.virtualApSecurityProfilePrefix = "SecurityProfile_";
  yrEngine.eoipTunnelPrefix = "eoipTunnel_";
  yrEngine.shipPhysicalWifiInterface = "shipPhysical";
  yrEngine.defaultPassword = "12345678";
  yrEngine.rootIpAddress = "10.90.";
```

# Issue #3 - no firewall

NMAP scan on the puplic IP

- Router os= Mikrotik Router OS
- Winbox Management 8291/TCP
- API access of the Yachtrouter exe 8728/TCP (API)

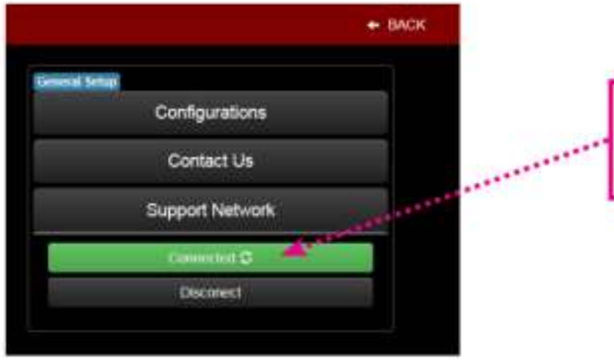
- Portscan from Internet:
- PORT     STATE SERVICE
- 21/tcp   open  ftp
- 22/tcp   open  ssh
- 53/tcp   open  domain
- 2000/tcp open  cisco-sccp
- 8291/tcp open  unknown



```
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.36.4 (c) 1999-2016       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level

[loco@YachtRouterBooster] > ls
```

# Issue #4 - Remote support

- **9.1. Remote Support**
  Each Yacht Router is equipped with Remote Support feature that gives our Technical Support ability to connect remotely over the Internet to your Yacht Router. You can use Remote Support
  in various situatons like remote setup, diagnostcs or Cloud Service actvaton.
-
  To establish Remote Support please send an e-mail to support@locomarine.com with following details:
  • Contact details (name, e-mail, phone number)
  • Yacht Router model
  • Yacht Router serial number
  • Descripton of the problem
  • Suggested best time (minimum one)



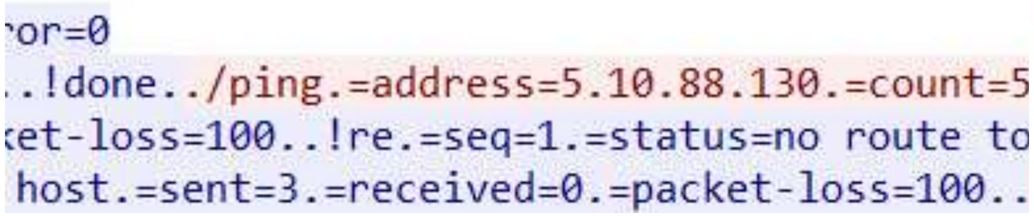
Click on **Connect** button to connect Yacht Router to Support Network. Once it is successfully connected button will go green.

# Issue #4 - Remote support

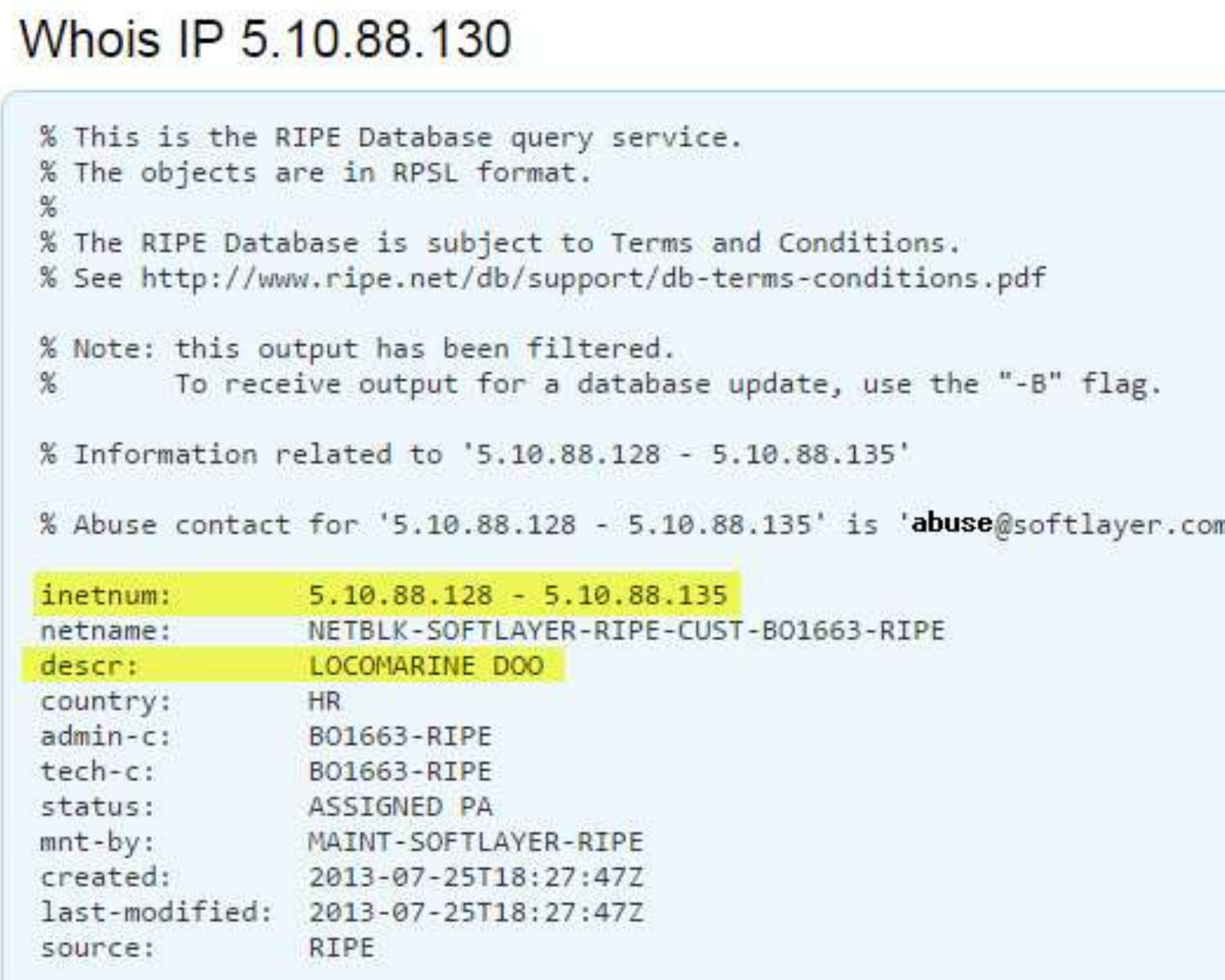
Yacht Router model & serial number ?

How do they know the IP address?

# Issue #4 - Remote support



```
ror=0
..!done../ping.=address=5.10.88.130.=count=5
ket-loss=100..!re.=seq=1.=status=no route to
 host.=sent=3.=received=0.=packet-loss=100..
```



Whois IP 5.10.88.130

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '5.10.88.128 - 5.10.88.135'

% Abuse contact for '5.10.88.128 - 5.10.88.135' is 'abuse@softlayer.com

inetnum:        5.10.88.128 - 5.10.88.135
netname:        NETBLK-SOFTLAYER-RIPE-CUST-BO1663-RIPE
descr:          LOCOMARINE DOO
country:        HR
admin-c:        BO1663-RIPE
tech-c:         BO1663-RIPE
status:         ASSIGNED PA
mnt-by:         MAINT-SOFTLAYER-RIPE
created:        2013-07-25T18:27:47Z
last-modified:  2013-07-25T18:27:47Z
source:         RIPE
```

## Issue #4 - Remote support

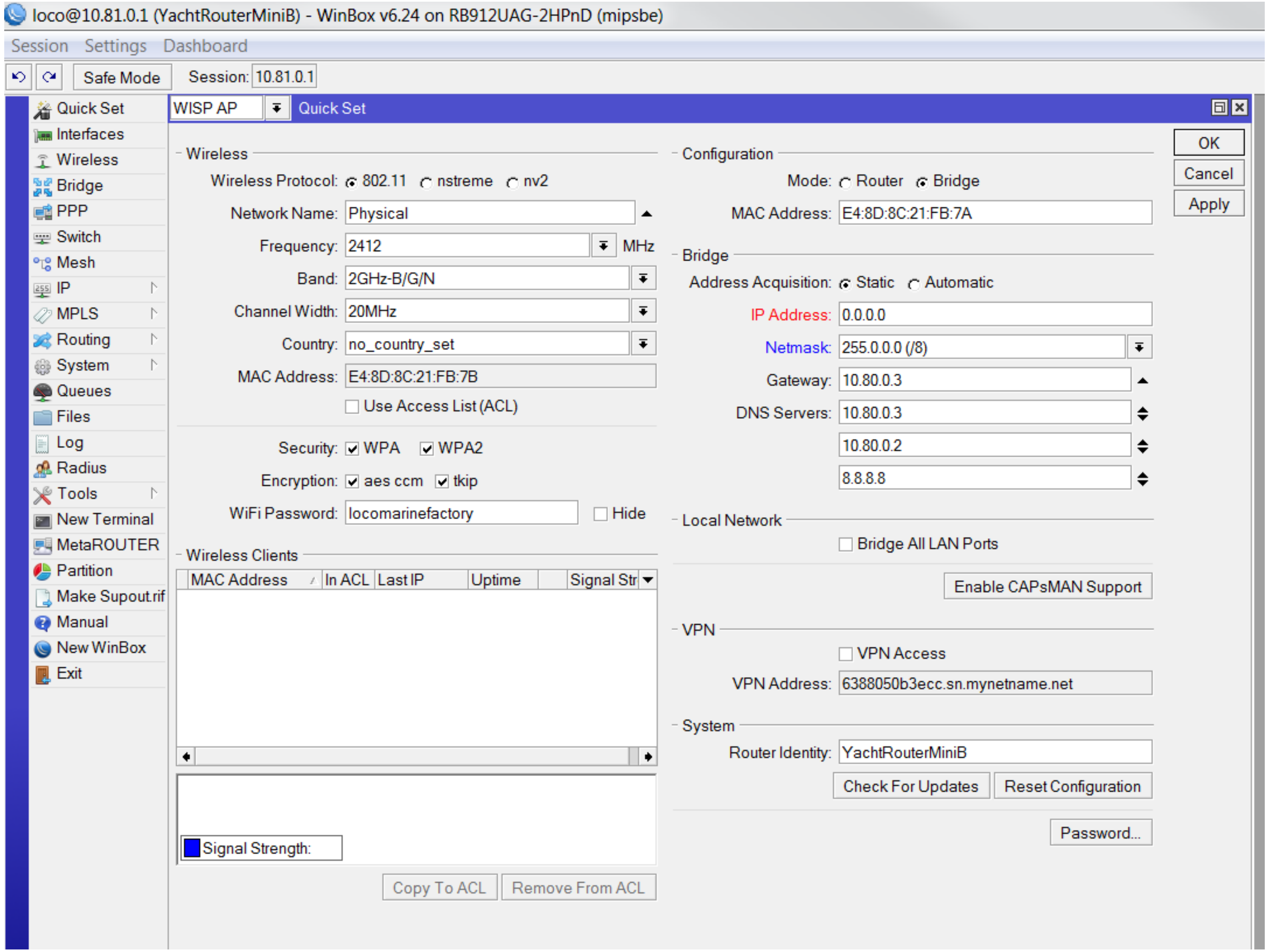
Remember the Portscan ?

Router os= Mikrotik Router OS
8291/tcp open  unknown

Port 8291/TCP belongs to Winbox Management

Ok, lets Try with the passwords from the source

# Issue #4 – WinBox Management



loco@10.81.0.1 (YachtRouterMiniB) - WinBox v6.24 on RB912UAG-2HPnD (mipsbe)

Session: 10.81.0.1

WISP AP Quick Set

Wireless

Wireless Protocol: ● 802.11 ○ nstreme ○ nv2

Network Name: Physical

Frequency: 2412 MHz

Band: 2GHz-B/G/N

Channel Width: 20MHz

Country: no_country_set

MAC Address: E4:8D:8C:21:FB:7B

□ Use Access List (ACL)

Security: ☑ WPA ☑ WPA2

Encryption: ☑ aes ccm ☑ tkip

WiFi Password: locomarinefactory □ Hide

Wireless Clients

| MAC Address | In ACL | Last IP | Uptime | Signal Str |
|---|---|---|---|---|

Signal Strength:

Configuration

Mode: ○ Router ● Bridge

MAC Address: E4:8D:8C:21:FB:7A

Bridge

Address Acquisition: ● Static ○ Automatic

IP Address: 0.0.0.0

Netmask: 255.0.0.0 (/8)

Gateway: 10.80.0.3

DNS Servers: 10.80.0.3
10.80.0.2
8.8.8.8

Local Network

□ Bridge All LAN Ports

VPN

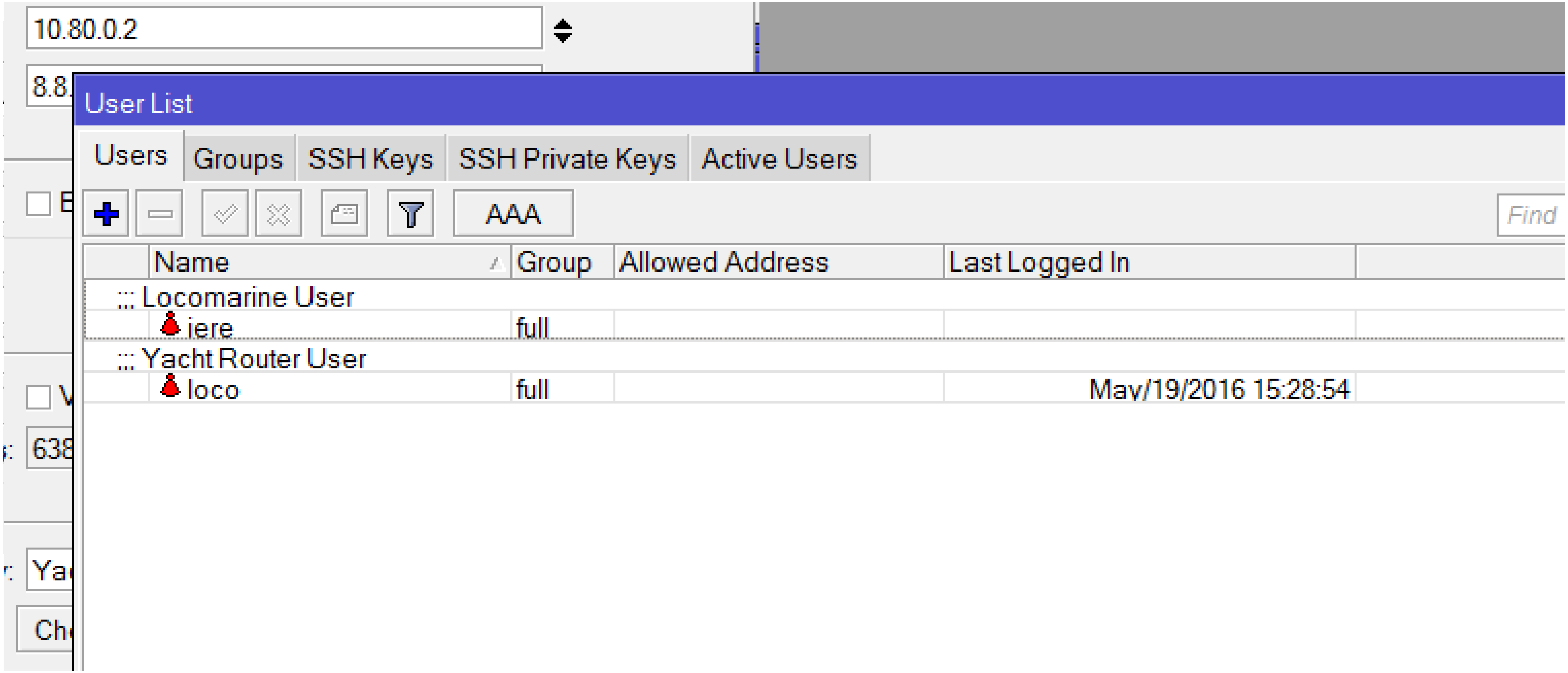
□ VPN Access

VPN Address: 6388050b3ecc.sn.mynetname.net

System

Router Identity: YachtRouterMiniB

# Issue #4 – Winbox Management



10.80.0.2

8.8.

638

Ya

| Name | Group | Allowed Address | Last Logged In |
|---|---|---|---|
| ;;; Locomarine User | | | |
| jere | full | | |
| ;;; Yacht Router User | | | |
| loco | full | | May/19/2016 15:28:54 |

# Issue #4 – Winbox Management Cracking

MKBRUTUS v1.0.0

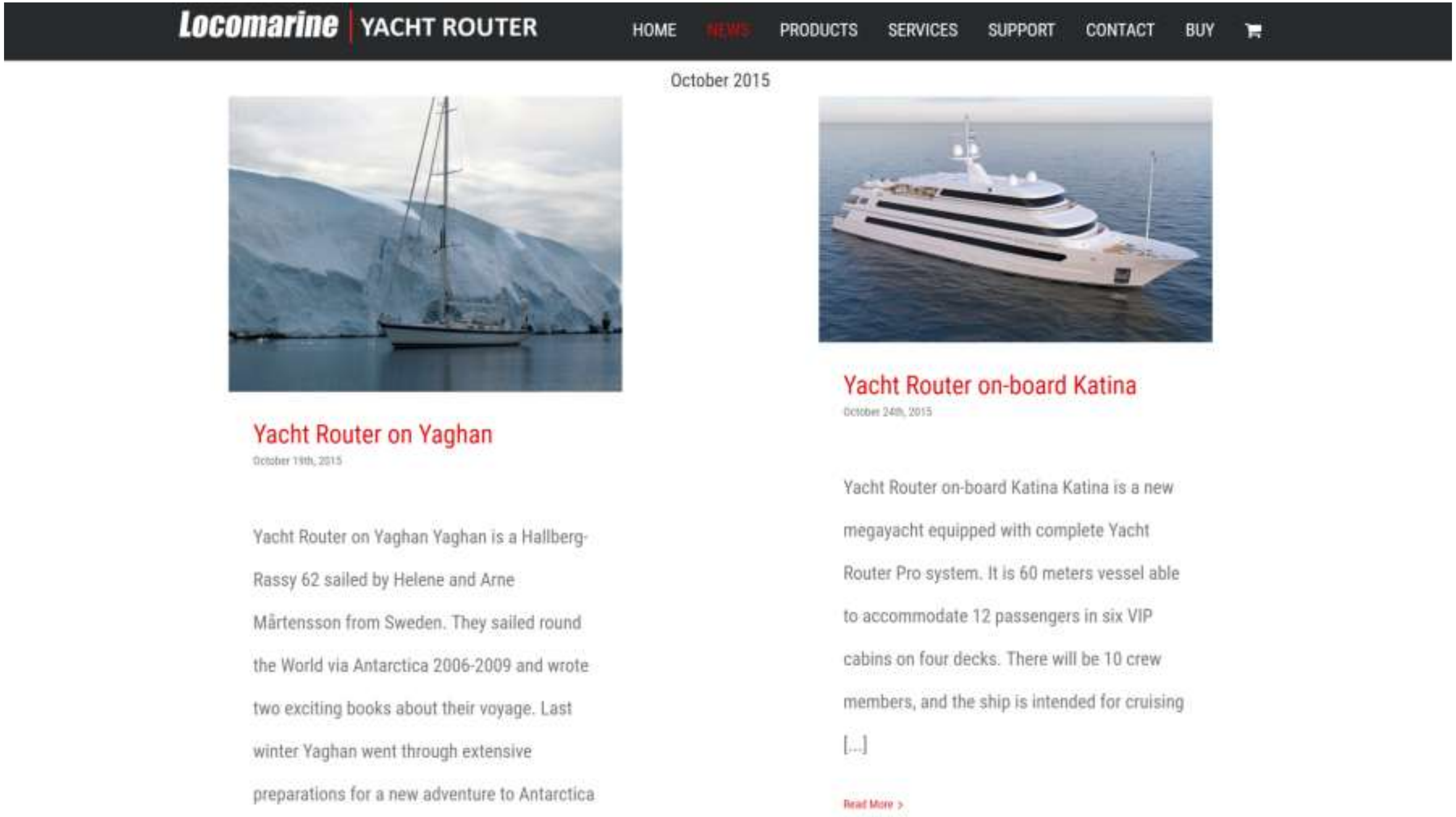
Password bruteforcer for MikroTik devices or boxes running RouterOS
Site: https://github.com/mkbrutusproject/MKBRUTUS

Or use CVE-2018-14847
https://github.com/BigNerd95/WinboxExploit

```
$ python3 WinboxExploit.py 192.168.0.1
```

- User: the user
- Pass: StrengGeheim

# How to find vulnerable Yachts



October 2015

Yacht Router on Yaghan

October 19th, 2015

Yacht Router on Yaghan Yaghan is a Hallberg-Rassy 62 sailed by Helene and Arne Mårtensson from Sweden. They sailed round the World via Antarctica 2006-2009 and wrote two exciting books about their voyage. Last winter Yaghan went through extensive preparations for a new adventure to Antarctica

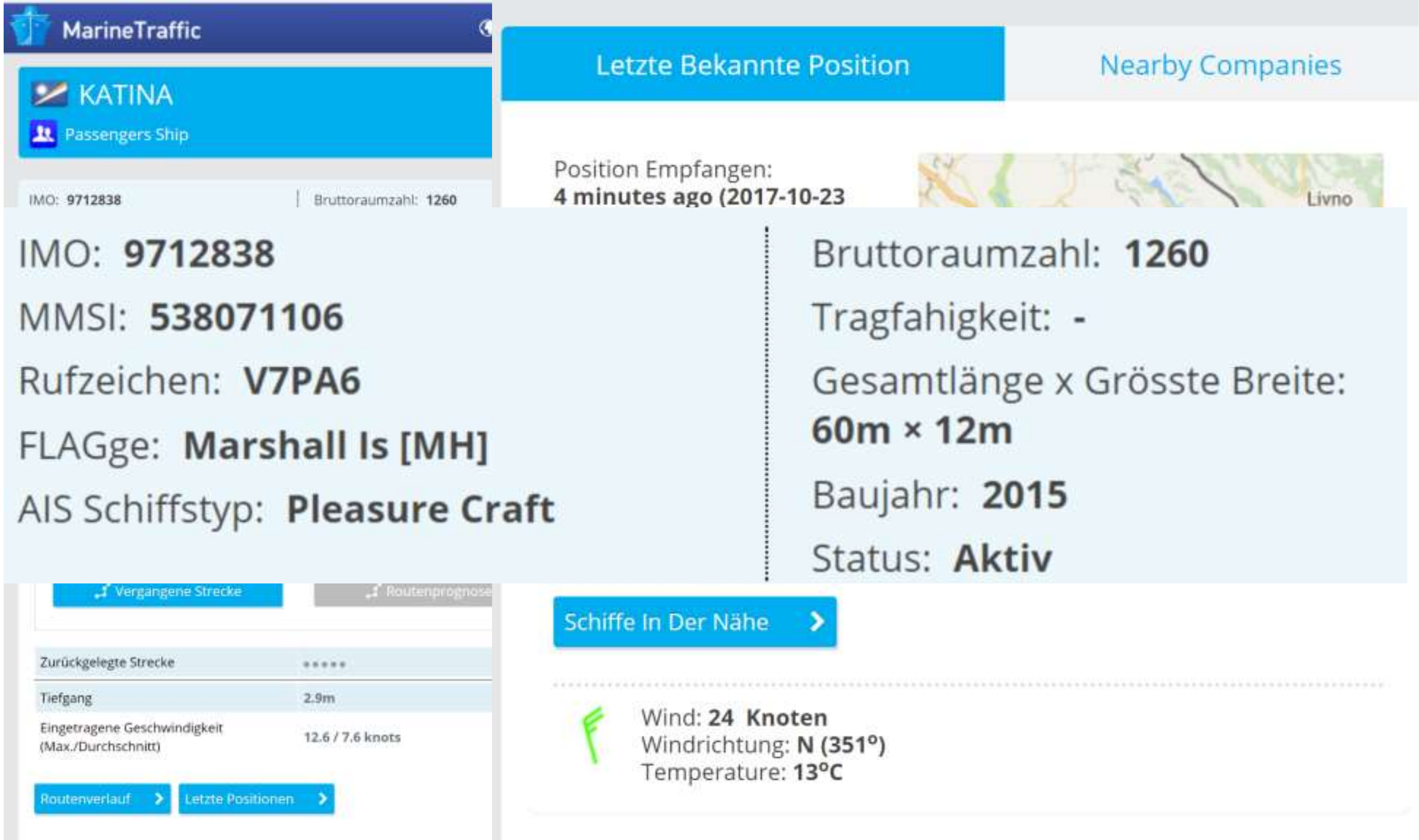
Yacht Router on-board Katina

October 24th, 2015

Yacht Router on-board Katina Katina is a new megayacht equipped with complete Yacht Router Pro system. It is 60 meters vessel able to accommodate 12 passengers in six VIP cabins on four decks. There will be 10 crew members, and the ship is intended for cruising [...]

Read More >

# How to find vulnerable Yachts



MarineTraffic

KATINA

Passengers Ship

IMO: 9712838 | Bruttoraumzahl: 1260

Letzte Bekannte Position | Nearby Companies

Position Empfangen:
**4 minutes ago (2017-10-23**

IMO: **9712838**

MMSI: **538071106**

Rufzeichen: **V7PA6**

FLAGge: **Marshall Is [MH]**

AIS Schiffstyp: **Pleasure Craft**

Bruttoraumzahl: **1260**

Tragfahigkeit: **-**

Gesamtlänge x Grösste Breite: **60m × 12m**

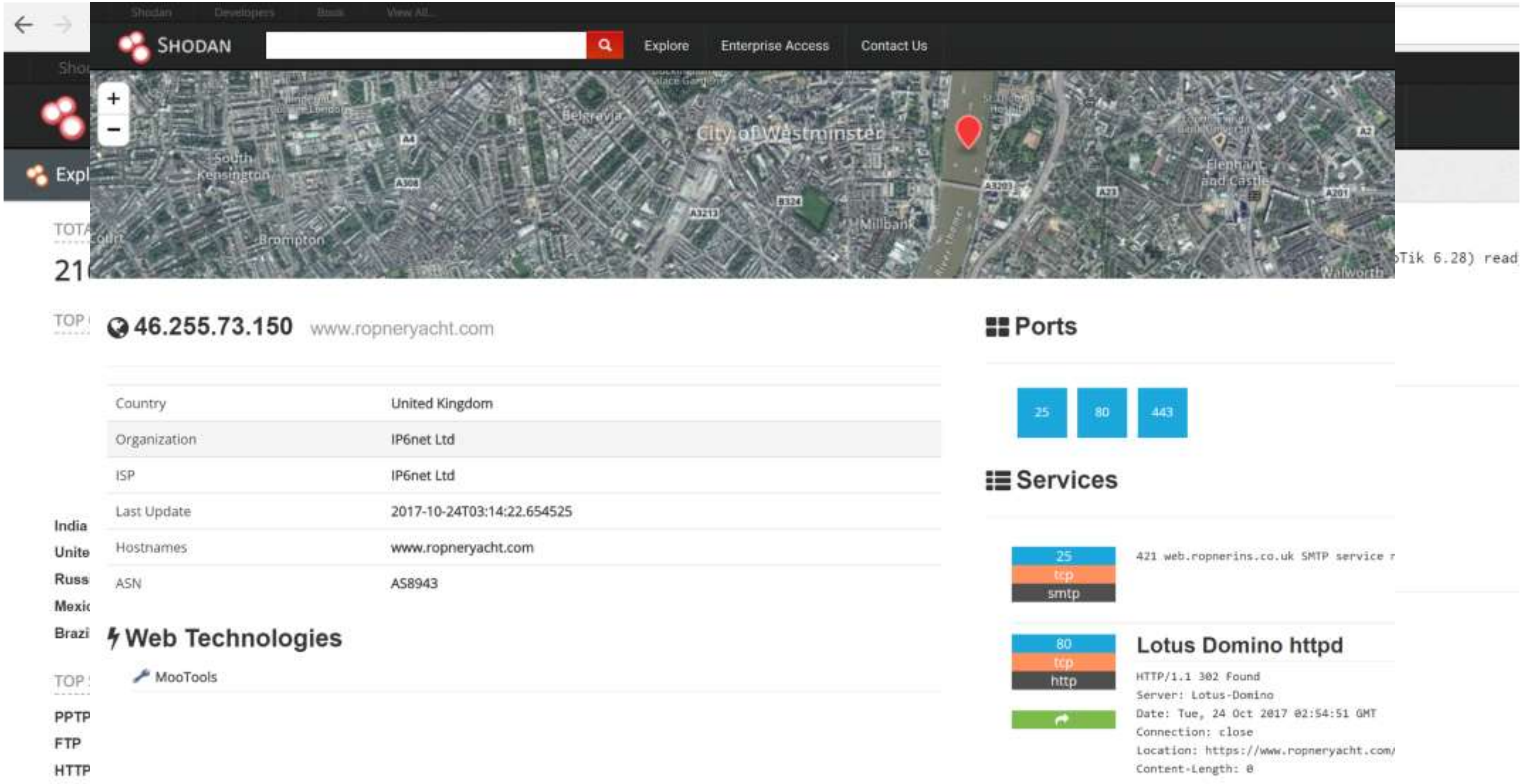
Baujahr: **2015**

Status: **Aktiv**

| | |
|---|---|
| Zurückgelegte Strecke | ***** |
| Tiefgang | 2.9m |
| Eingetragene Geschwindigkeit (Max./Durchschnitt) | 12.6 / 7.6 knots |

Wind: **24 Knoten**
Windrichtung: **N (351°)**
Temperature: **13°C**

# How to find vulnerable Yachts



**46.255.73.150** www.ropneryacht.com

| | |
|---|---|
| Country | United Kingdom |
| Organization | IP6net Ltd |
| ISP | IP6net Ltd |
| Last Update | 2017-10-24T03:14:22.654525 |
| Hostnames | www.ropneryacht.com |
| ASN | AS8943 |

**Web Technologies**

MooTools

**Ports**

25 80 443

**Services**

25 tcp smtp

```
421 web.ropnerins.co.uk SMTP service r
```

80 tcp http

**Lotus Domino httpd**

```
HTTP/1.1 302 Found
Server: Lotus-Domino
Date: Tue, 24 Oct 2017 02:54:51 GMT
Connection: close
Location: https://www.ropneryacht.com/
Content-Length: 0
```

# Vendor response

- Security issues reported in June 2017 to vendor
- 2 bugs intensely fixed
- New Apps and router firmware versions were developed
- In November finaly released
- Permission from vendor to present
- CVE-2017-17673 requested

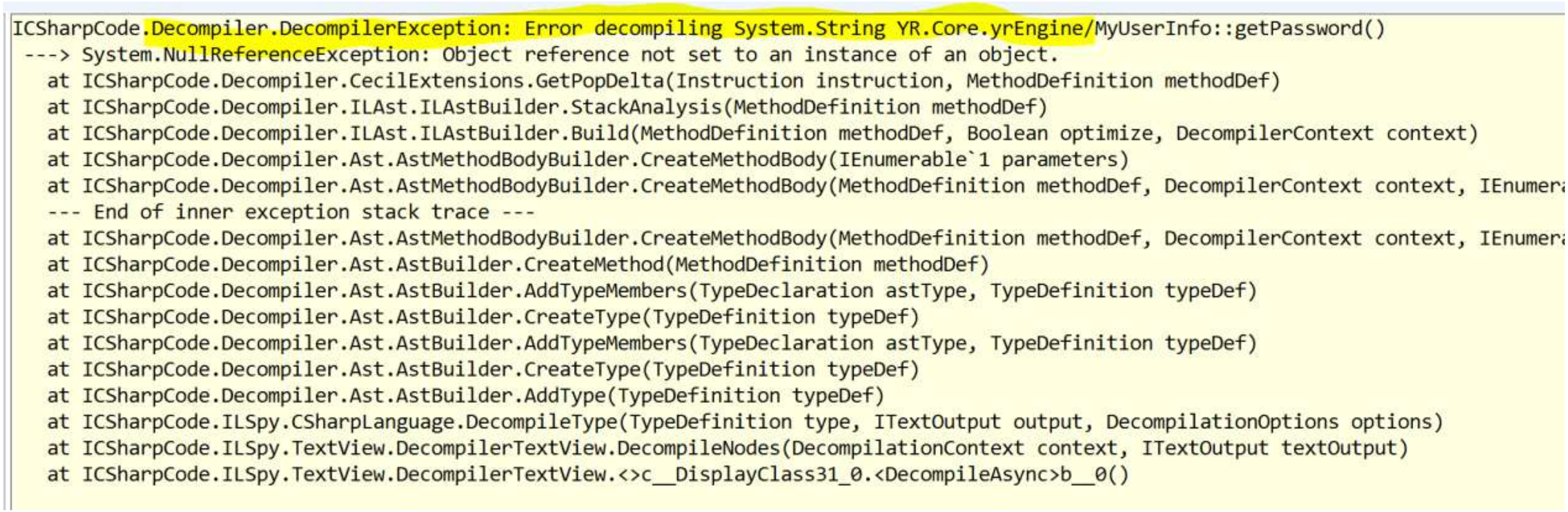
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17673

# Testing of the patched Software

- Vendor asked me to test the patched software
- They send me a Test Router
- .Net application is now obfuscated
- SSH instead of FTP

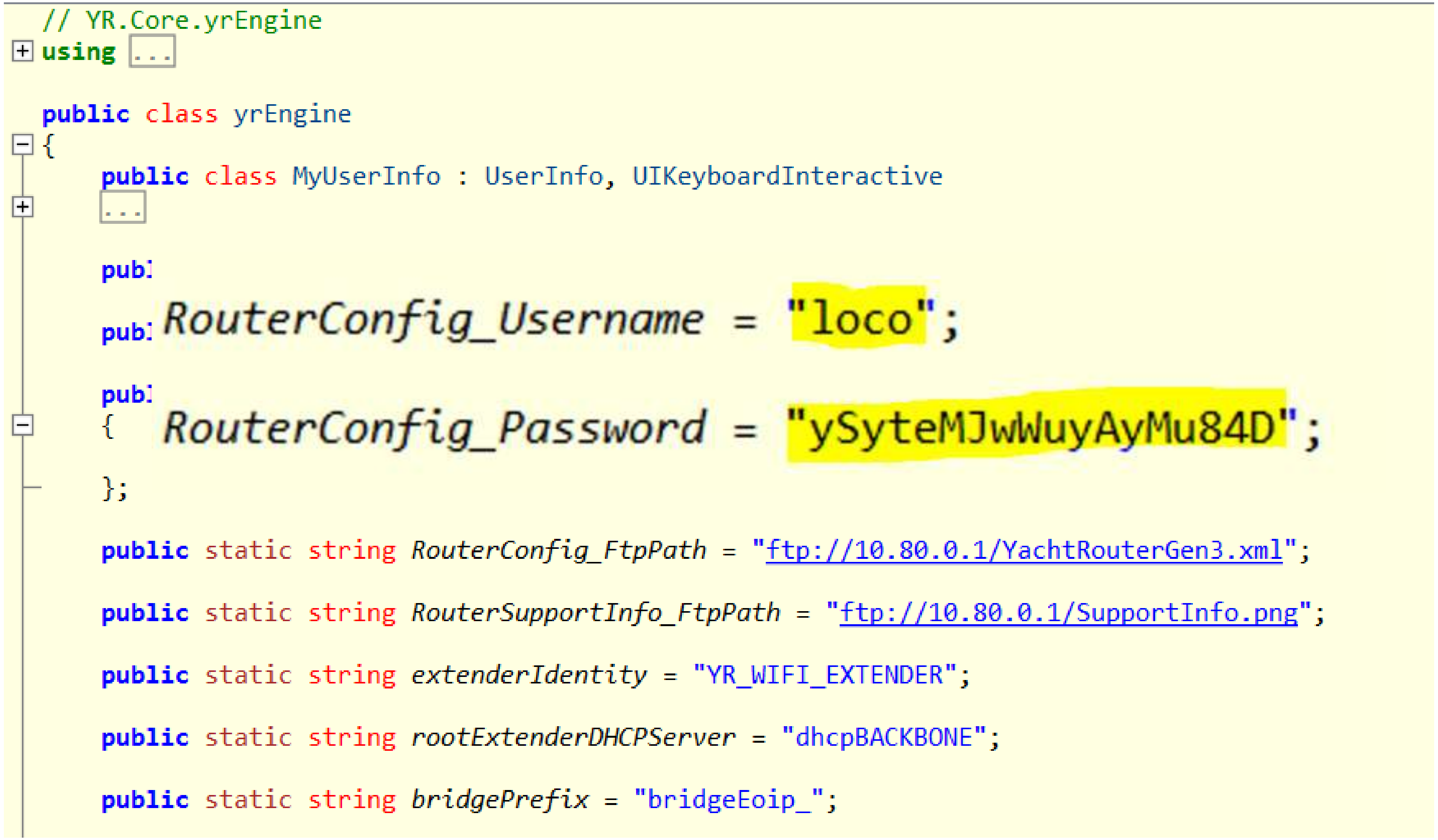
But…. Security by obscurity – seriously ?

# Testing of the patched Software



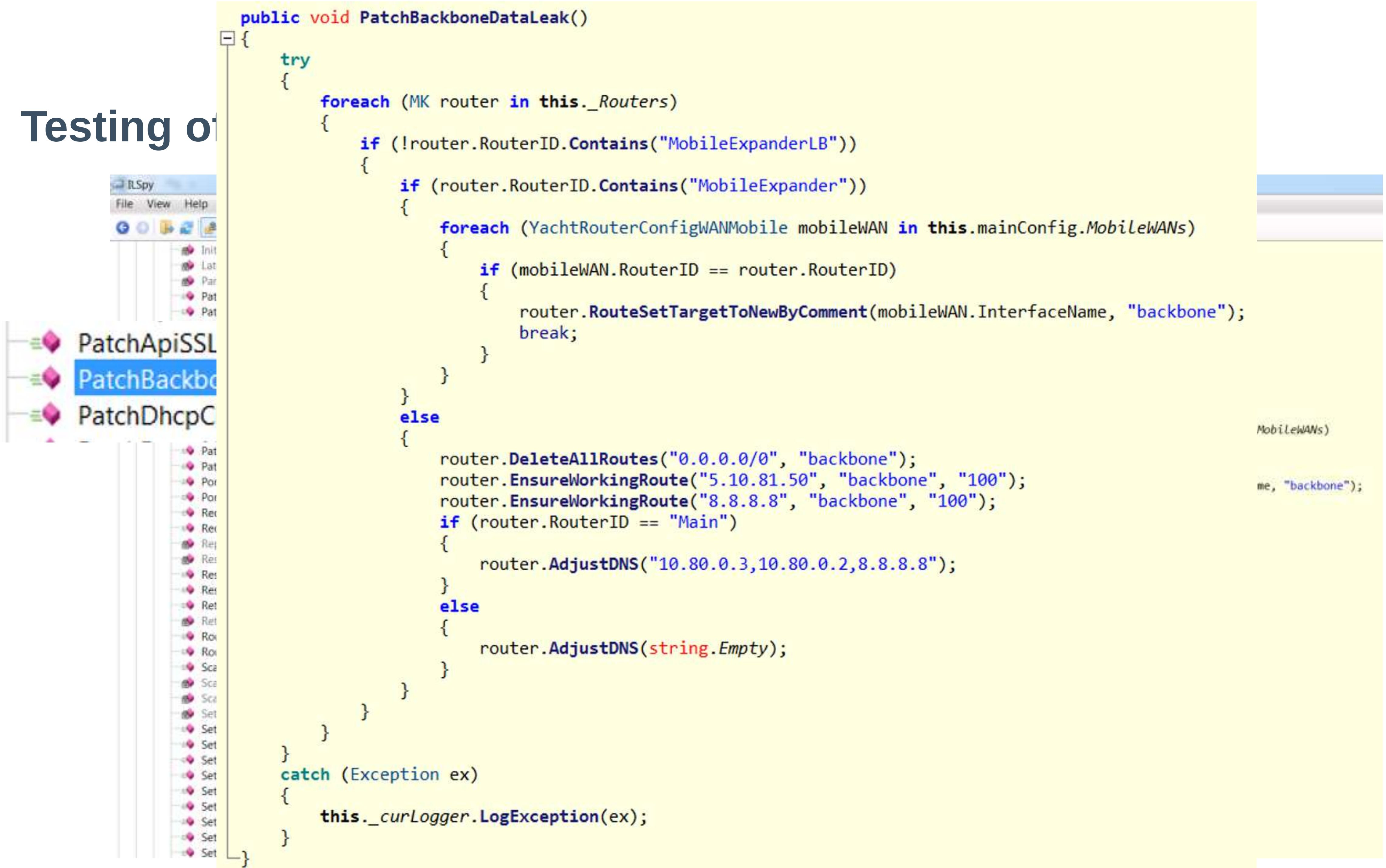
```
ICSharpCode.Decompiler.DecompilerException: Error decompiling System.String YR.Core.yrEngine/MyUserInfo::getPassword()
 ---> System.NullReferenceException: Object reference not set to an instance of an object.
   at ICSharpCode.Decompiler.CecilExtensions.GetPopDelta(Instruction instruction, MethodDefinition methodDef)
   at ICSharpCode.Decompiler.ILAst.ILAstBuilder.StackAnalysis(MethodDefinition methodDef)
   at ICSharpCode.Decompiler.ILAst.ILAstBuilder.Build(MethodDefinition methodDef, Boolean optimize, DecompilerContext context)
   at ICSharpCode.Decompiler.Ast.AstMethodBodyBuilder.CreateMethodBody(IEnumerable`1 parameters)
   at ICSharpCode.Decompiler.Ast.AstMethodBodyBuilder.CreateMethodBody(MethodDefinition methodDef, DecompilerContext context, IEnumera
   --- End of inner exception stack trace ---
   at ICSharpCode.Decompiler.Ast.AstMethodBodyBuilder.CreateMethodBody(MethodDefinition methodDef, DecompilerContext context, IEnumera
   at ICSharpCode.Decompiler.Ast.AstBuilder.CreateMethod(MethodDefinition methodDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.AddTypeMembers(TypeDeclaration astType, TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.CreateType(TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.AddTypeMembers(TypeDeclaration astType, TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.CreateType(TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.AddType(TypeDefinition typeDef)
   at ICSharpCode.ILSpy.CSharpLanguage.DecompileType(TypeDefinition type, ITextOutput output, DecompilationOptions options)
   at ICSharpCode.ILSpy.TextView.DecompilerTextView.DecompileNodes(DecompilationContext context, ITextOutput textOutput)
   at ICSharpCode.ILSpy.TextView.DecompilerTextView.<>c__DisplayClass31_0.<DecompileAsync>b__0()
```

# Don‘t forget the APP‘s



```
// YR.Core.yrEngine
using ...

public class yrEngine
{
    public class MyUserInfo : UserInfo, UIKeyboardInteractive
    ...

    publ
    publ RouterConfig_Username = "loco";

    publ
    {    RouterConfig_Password = "ySyteMJwWuyAyMu84D";

    };

    public static string RouterConfig_FtpPath = "ftp://10.80.0.1/YachtRouterGen3.xml";

    public static string RouterSupportInfo_FtpPath = "ftp://10.80.0.1/SupportInfo.png";

    public static string extenderIdentity = "YR_WIFI_EXTENDER";

    public static string rootExtenderDHCPServer = "dhcpBACKBONE";

    public static string bridgePrefix = "bridgeEoip_";
```

# Testing of



```
public void PatchBackboneDataLeak()
{
    try
    {
        foreach (MK router in this._Routers)
        {
            if (!router.RouterID.Contains("MobileExpanderLB"))
            {
                if (router.RouterID.Contains("MobileExpander"))
                {
                    foreach (YachtRouterConfigWANMobile mobileWAN in this.mainConfig.MobileWANs)
                    {
                        if (mobileWAN.RouterID == router.RouterID)
                        {
                            router.RouteSetTargetToNewByComment(mobileWAN.InterfaceName, "backbone");
                            break;
                        }
                    }
                }
                else
                {
                    router.DeleteAllRoutes("0.0.0.0/0", "backbone");
                    router.EnsureWorkingRoute("5.10.81.50", "backbone", "100");
                    router.EnsureWorkingRoute("8.8.8.8", "backbone", "100");
                    if (router.RouterID == "Main")
                    {
                        router.AdjustDNS("10.80.0.3,10.80.0.2,8.8.8.8");
                    }
                    else
                    {
                        router.AdjustDNS(string.Empty);
                    }
                }
            }
        }
    }
    catch (Exception ex)
    {
        this._curLogger.LogException(ex);
    }
}
```

# Summery of the Patches

- Use of SSH instead of FTP
- Obfuscated Exe + DLL in Windows Version
- Android APK not obfuscated
- iOS Version not tested yest
- still Hardcoded credentials in yrEngine
- SSH and Winbox still reachable from Internet

# Satcom

# Satcom

- Offshore internet acces via Satcom
- Patching ?
- Many old Versions still online
- A sample

# Satcom

Shodan.io search hint’s for possible vulnerable devices

- “Sailor 900”
- “Inmarsat Solutions”
- “Telenor Satellite”
- “Commbox”
- org:"Intelsat GlobalConnex Solutions (GXS)“
- org:"Telenor UK Ltd"

# Satcom

Did u know? Shodan.io has a Live Shiptracker

URL: Shiptracker.shodan.io

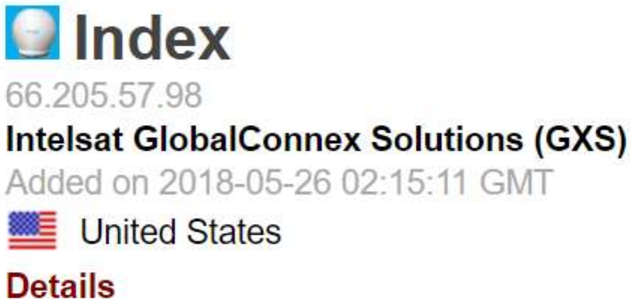
Tracks via VSAT connected Antennas and exposes Web Services

# Satcom

Was shodan surfing for other Satcom Boxes !

Digital Antenna System paid my attention

- Results in Cobham MXP Webserver
- Shodan Query for “Server: Micro Digital Webserver” gives result



**Index**

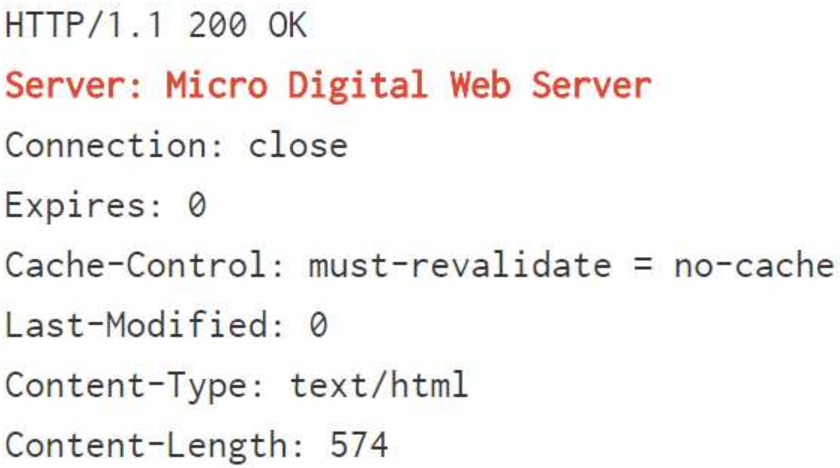
66.205.57.98

**Intelsat GlobalConnex Solutions (GXS)**

Added on 2018-05-26 02:15:11 GMT

🇺🇸 United States

**Details**

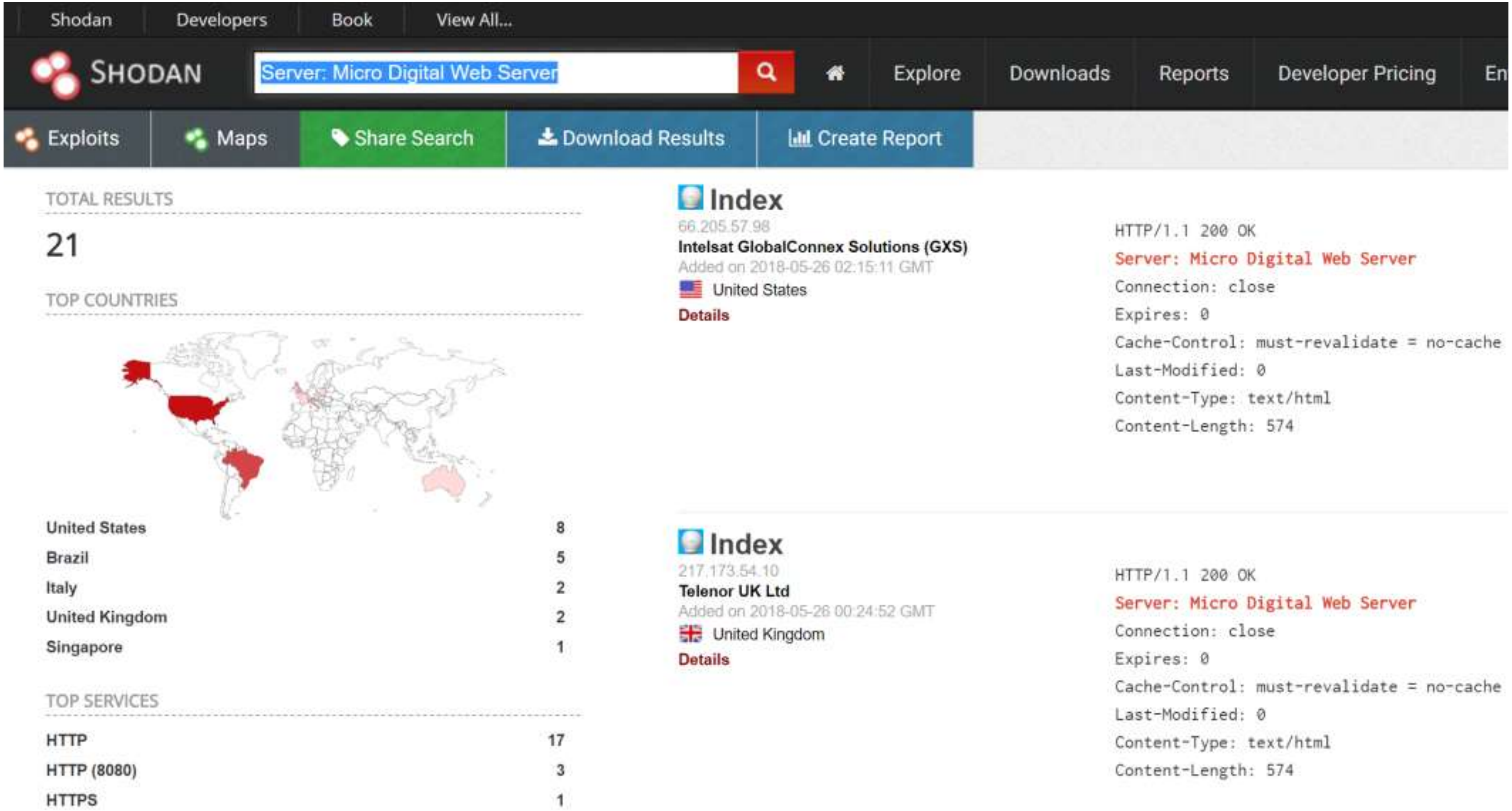


```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Expires: 0
Cache-Control: must-revalidate = no-cache
Last-Modified: 0
Content-Type: text/html
Content-Length: 574
```

# Cobham Seatel Satcom

Demo

# Search “Server: Micro Digital Webserver”



TOTAL RESULTS

21

TOP COUNTRIES

| | |
|---|---|
| United States | 8 |
| Brazil | 5 |
| Italy | 2 |
| United Kingdom | 2 |
| Singapore | 1 |

TOP SERVICES

| | |
|---|---|
| HTTP | 17 |
| HTTP (8080) | 3 |
| HTTPS | 1 |

**Index**

66.205.57.98

**Intelsat GlobalConnex Solutions (GXS)**

Added on 2018-05-26 02:15:11 GMT

United States

**Details**

```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Expires: 0
Cache-Control: must-revalidate = no-cache
Last-Modified: 0
Content-Type: text/html
Content-Length: 574
```

**Index**

217.173.54.10

**Telenor UK Ltd**

Added on 2018-05-26 00:24:52 GMT

United Kingdom

**Details**

```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Expires: 0
Cache-Control: must-revalidate = no-cache
Last-Modified: 0
Content-Type: text/html
Content-Length: 574
```

# Cobham Seatel Satcom

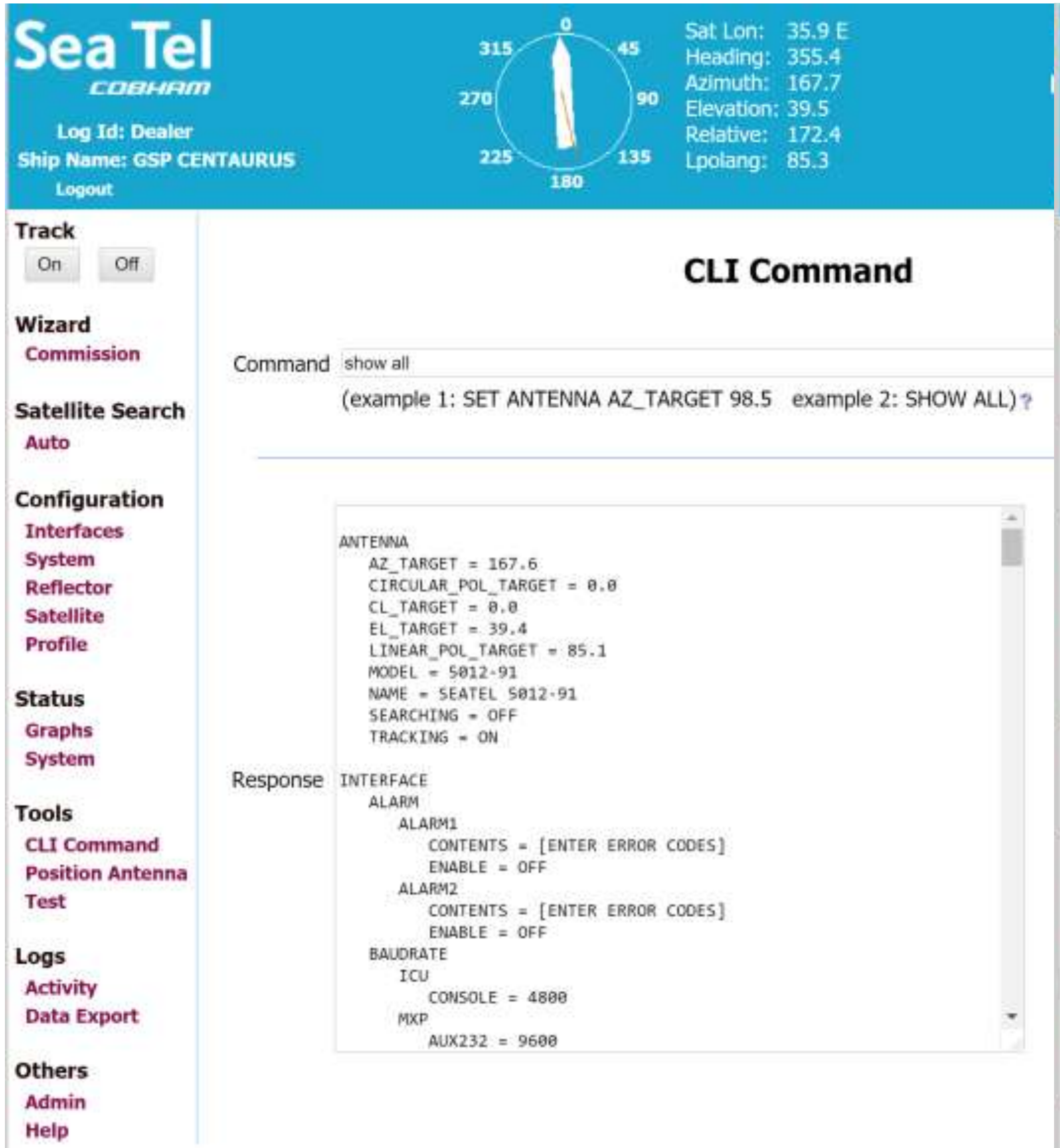
- Was looking for Satcom devices via Shodan
- Found some online
- Analyzed Webinterface with Fiddler/burpsuite
- Found some juicy javascripts

# Cobham Seatel Satcom

/js/userLogin.js contains some hints

```
if(t=="Dealer"){if(r=="true"){e="MenuDealerGx.html"}else{e="MenuDealer.html"}}else
if(t=="SysAdmin"){if(r=="true"){e="MenuSysGx.html"}else{e="MenuSys.html"}}else
if(t=="User"){if(r=="true"){e="MenuEuNCGx.html"}else{e="MenuEuNC.html"}}
```

# Cobham Seatel Satcom



Log Id: Dealer
Ship Name: GSP CENTAURUS

Sat Lon: 35.9 E
Heading: 355.4
Azimuth: 167.7
Elevation: 39.5
Relative: 172.4
Lpolang: 85.3

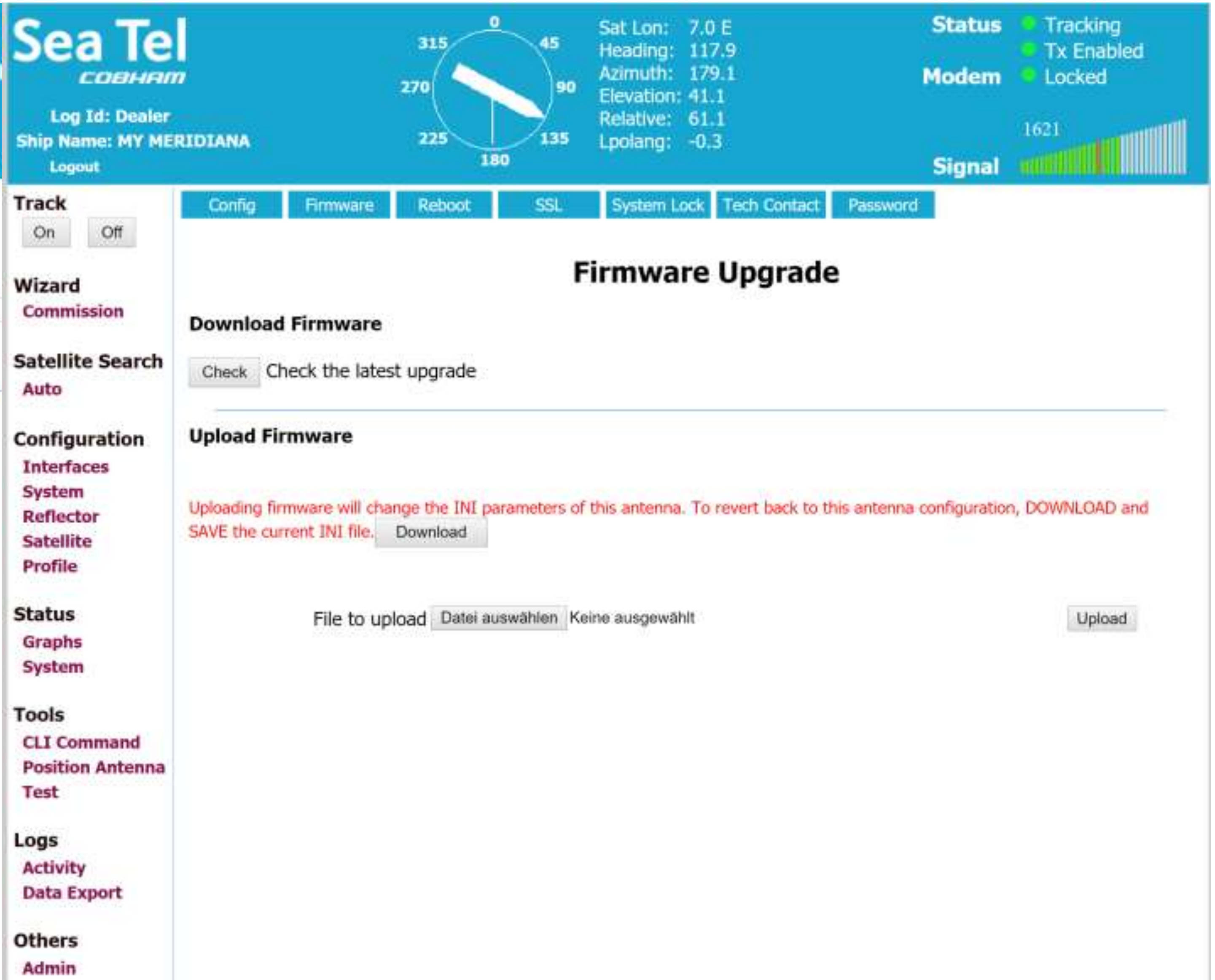
## CLI Command

Command: show all

(example 1: SET ANTENNA AZ_TARGET 98.5    example 2: SHOW ALL)

Response

```
ANTENNA
   AZ_TARGET = 167.6
   CIRCULAR_POL_TARGET = 0.0
   CL_TARGET = 0.0
   EL_TARGET = 39.4
   LINEAR_POL_TARGET = 85.1
   MODEL = 5012-91
   NAME = SEATEL 5012-91
   SEARCHING = OFF
   TRACKING = ON

INTERFACE
   ALARM
      ALARM1
         CONTENTS = [ENTER ERROR CODES]
         ENABLE = OFF
      ALARM2
         CONTENTS = [ENTER ERROR CODES]
         ENABLE = OFF
   BAUDRATE
      ICU
         CONSOLE = 4800
      MXP
         AUX232 = 9600
```



Log Id: Dealer
Ship Name: MY MERIDIANA

Sat Lon: 7.0 E
Heading: 117.9
Azimuth: 179.1
Elevation: 41.1
Relative: 61.1
Lpolang: -0.3

Status: ● Tracking
● Tx Enabled
Modem: ● Locked
Signal: 1621

## Firmware Upgrade

**Download Firmware**

Check the latest upgrade

**Upload Firmware**

Uploading firmware will change the INI parameters of this antenna. To revert back to this antenna configuration, DOWNLOAD and SAVE the current INI file.

File to upload: Keine ausgewählt

# Cobham Seatel Satcom RTFM

RTFM ! In the manual: default usename and password

- Dealer
- seatel3

- SysAdmin
- seatel2

- User
- seatel1

## Cobham Seatel Satcom

CVE Lookup if someone found already:

F..K – someone was already faster

But….

# Cobham Seatel Satcom

CVE-2018-5267 reported Auth bypass only in Version 121 Build 222701

I can confirm following other versions too:

- Version number: 179 (Build:224945)
- Version number: 171 (Build:224753)
- Version number: 148 (Build:223591)
- Version number: 147 (Build:223551)

## Cobham Seatel Satcom

To have fun with the seatel device, following Menues are available without authentication:

| | |
|---|---|
| ConfigPortGx.html | configuration der IO Ports |
| CommDiag.html | cli command interface |
| PositionAntGx.html | change Antenna configuration |
| FileAdmin.html | |
| CfgFileDnUpload.html | down/upload config |
| FirmwareUpload.html | firmware update |
| CfgSysCommon.html | rename ship name in menue |
| SysStatus.html | |
| RebootUnit.html | reboot |

# Cobham Seatel Satcom

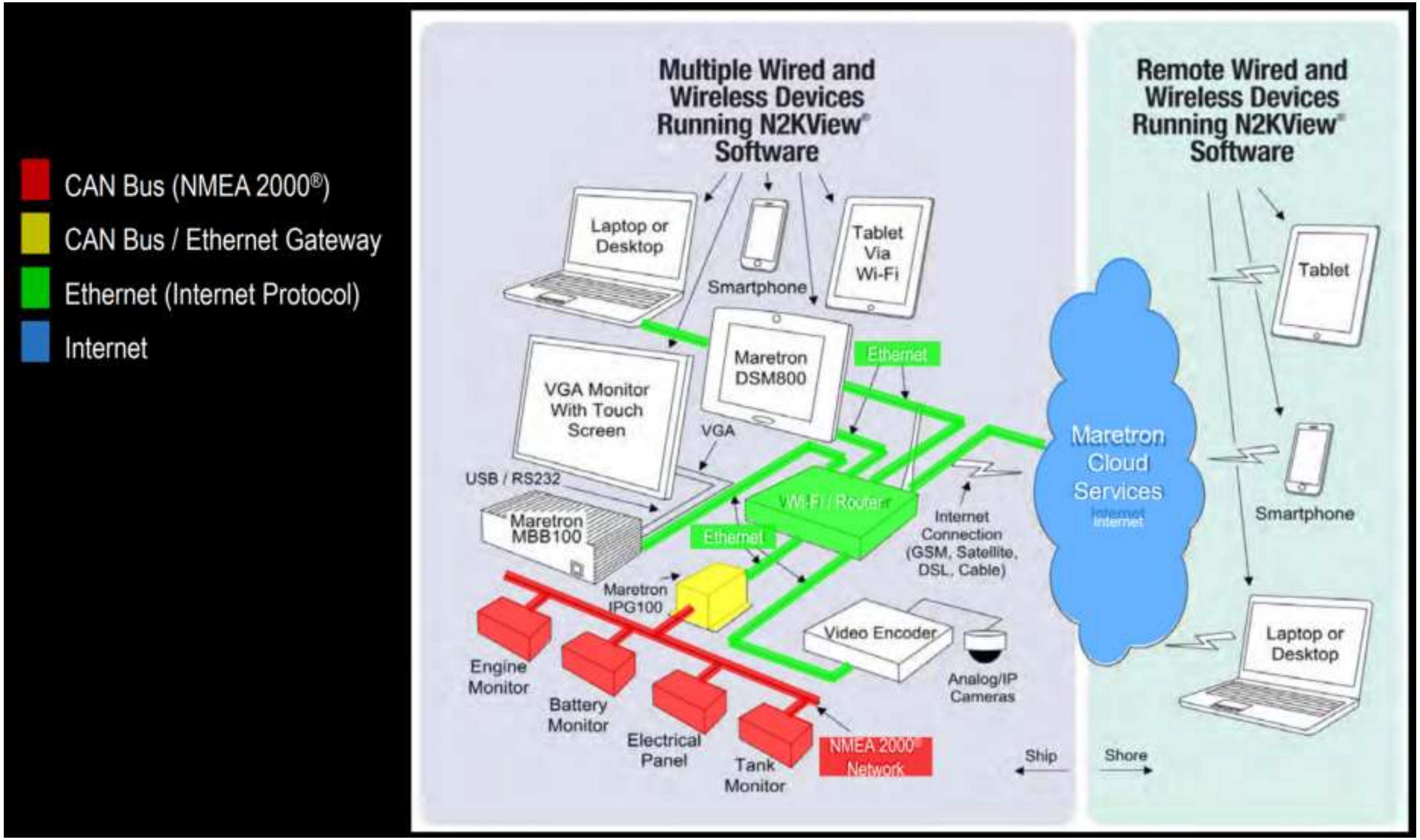
Whats the Risk now?

- Increase Cost
- Denial of Service

# What’s next?

- NMEA protocol needs more test
- Wireless Autopilot
- Other Internet Equipment tested by others
- Vessel hacking is just in the beginning
- Cloud services

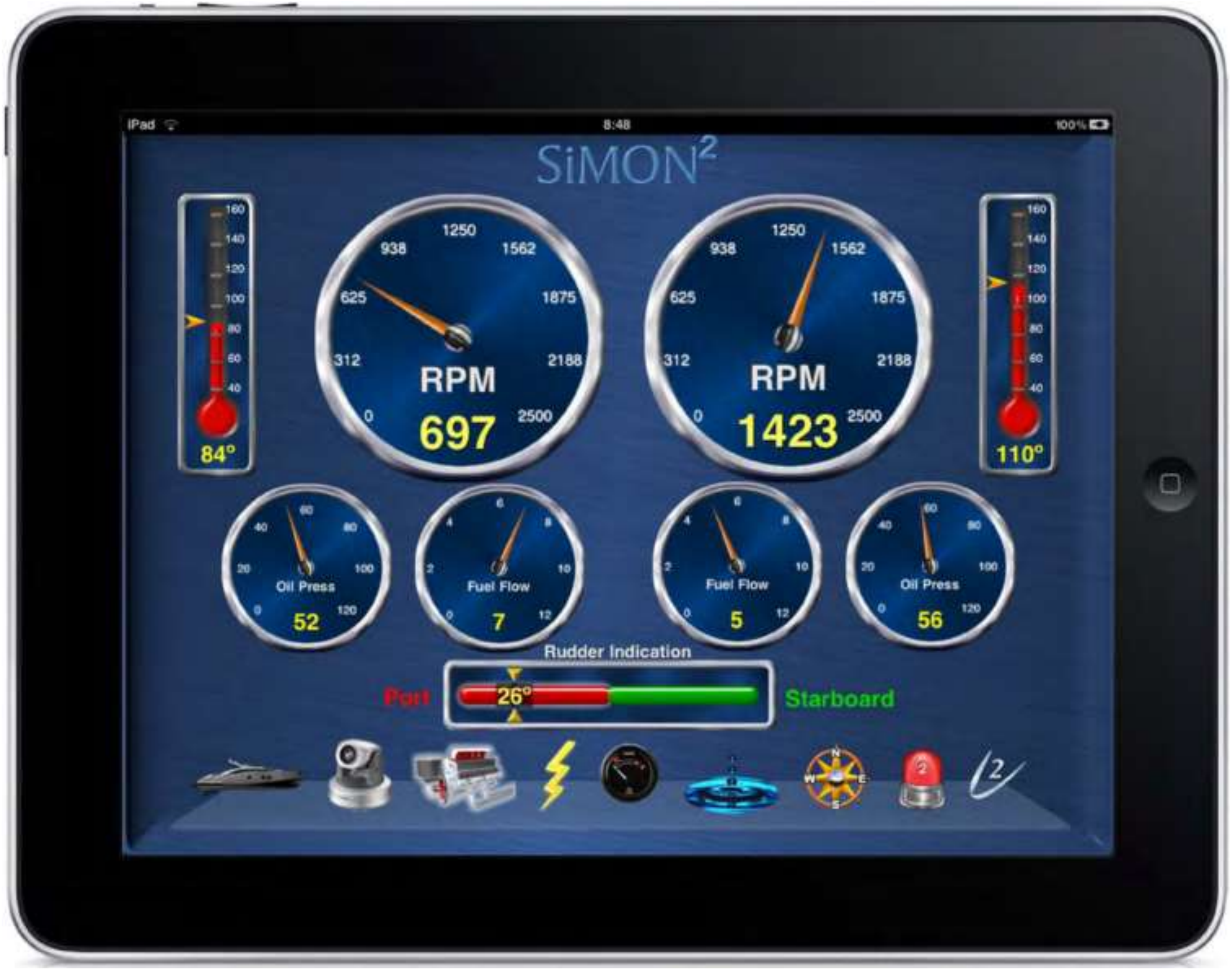
# Future is cloud



https://www.nmea.org/Assets/nmea%20ibex%20integrating%20smart%20phones%20%20marine%20electronics%20lr.pdf

# Cloud services

- Engine control
- Monitoring
- From anywhere



https://www.nmea.org/Assets/nmea%20ibex%20integrating%20smart%20phones%20%20marine%20electronics%20lr.pdf

# conclusion

- NMEA Gateways needs more research
- SATCom Boxes mostly unpatched
- VTS is unexplored
- Autopilot Remote control (currently working on)
- Injecting NMEA messages to the Bus (currently working on)
- GPS spoofing protection (DLR “Galant” new Antenna array)

My conclusion: Maritime Cyber-Security is years behind

May the force be with u

Twitter: @ObiWan666

SGerling@ROSEN-Group.com

# THANK YOU FOR JOINING THIS PRESENTATION.

www.certivation.com

CERTivation