CyberKeel

# Cyber Security Challenges

**June 2nd 2016**

Lars Jensen

*CEO*

CyberKeel

Lars.Jensen@CyberKeel.com

# Agenda

- Main types of threat vectors
- Overall landscape of threat actors
- Likelihood and consequences of attacks
- Risk mitigation – what should be done?

# Current state of affairs in the maritime sector

- The level of cyber security remains at a low level in the maritime industry – Awareness is becoming high with IT staff, but there is still a way to go with senior management

- Attacks are happening

- Patch and update procedures are slow on the landside and extremely haphazard on the seaside

- State-of-the-art firewall and anti-virus software is ineffective in keeping out dedicated attacks

- Social engineering tactics work very well

- When we talk to the IT departments they often give the impression that they do not see the necessary support and understanding of the issue from senior management

- US DHS: “Unless cyber vulnerabilities are addressed, they will pose a significant risk to port facilities and aboard vessels within the Maritime Subsector”

# But is there a problem – in reality?

# But first: a brief look at actual maritime or maritime-related incidents

- Port operations disrupted in US Port due to GPS jamming
- (Old example) Port of Antwerp smuggling case
- High-level port study of Danish ports show 80% of ports appear vulnerable to simple intrusion tools
- Ships with “email access only” are not “email access only”
- Little to no Cyber security policy and guideline in daily work on vessels
- Critical systems running on Windows XP
- Critical systems running on exposed computers
- AIS spoofing and manipulation
- Confidential vessel owner information exposed to the charterer
- USS Guardian (mine countermeasure ship) ran aground in 2013 due to inaccurate nautical charts. Vessel worth 277m USD lost. Not a cyber attack per se, but shows the risk of ECDIS manipulation.
- Remote navigation of an 80 million dollar yacht using 3000 USD worth of equipment
- Facebook as pirate intelligence source
- Floating platform tilted slightly due to cyber attack

# Helpful examples from other industries

- Stuxnet virus targeting industrial control systems in Iran which were not online
- Successful hacking of cars
- Shut-down of powerplant in Ukraine – same approach unsuccessfully used against Kiev Airport
- Hacking of a steel mill to overload blast furnace in Germany

# Bad news: Shodan, your hardware is visible

Search engine for available connections on the internet.

-Webcams.

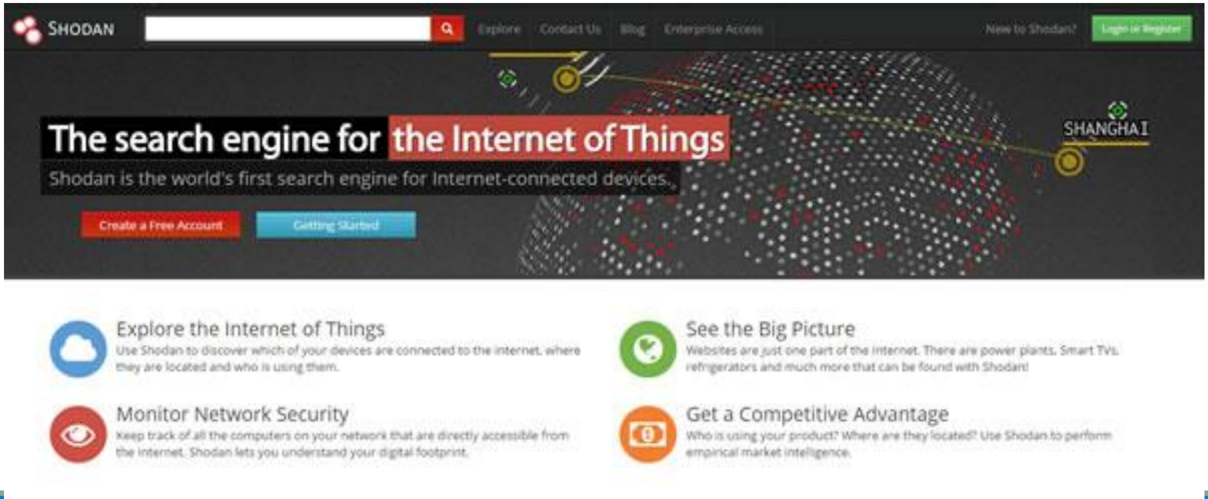
-Traffic lights.

-Servers.

Database update is performed by Shodan

-No attacker fingerprint

-May match systems against available exploits or known passwords



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

# Worse news: make a targeted search

If you know which specific hardware component you are searching for, you can – literally – search the entire internet within a day

# Threat actors – what is the purpose?

- Commercial Key actors: Criminals
  - Denial-of-asset / cyber-piracy
    - Ransomware
    - Jamming
  - Cost impact on competitors
- Military Key actors: Nation states or state-sponsored groups
  - Espionage
  - Denial-of-asset / destruction of asset
- Terrorism Key actors: self-proclaimed “groups” or state-sponsored groups
  - Denial-of-asset / destruction of asset
  - Publicity / cause “spectacular” damage such as loss of life, environmental spills etc
- No purpose Key actors: staff
  - Malware overload due to negligence
  - Disruptions due to incompetence

# Risk mitigation

- Be realistic – have a strong contingency plan
- Improve staff awareness – both to detect and defend
- Improve patch and update procedures
- Establish – and enforce – system separation

# It doesn’t have to be difficult….