Attaques CYBER 2020

Le secteur maritime particulièrement touché

International Maritime Organization
79 323 abonnés
4 h · Modifié ·

A number of IMO's web-based services are currently unavailable, including IMO's public website. Service has been restored to the GISIS database, IMODOCS and Virtual Publications. The interruption of service was caused by a sophisticated cyber attack against the Organization's IT systems that overcame robust security measures in place. IMO IT technicians shut down key systems to prevent further damage from the attack. The IMO is working with UN IT and security experts to restore systems as soon as possible, identify the source of the attack, and further enhance security systems to prevent recurrence.

Voir la traduction

Suspecting Cyber Attack, MSC Reports Network Outage – Update

April 10, 2020 by Mike Schuler

Mars 2020 – Suisse (MSC)

Janvier 2020 – Elbe (Spoofing AIS)

EUROPEAN COAST GUARD FUNCTIONS FORUM

March 2020 UNCLASS – For Official Use Only

Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks (NY Times May 19)

Israel was behind a cyberattack that disrupted a major port in Iran, done in response to an attempt by the Revolutionary Guards to infiltrate an Israeli water facility.

Avril 2020 – Ormuz Pot de Bandar Abbas (Attaque ISR)

Sept 2020 – Int (CMA-CGM)

Mai 2020 – Californie (Spoofing AIS)

Sept 2020 – Int (GEFCO)

Med Europe Terminal

Actualités

/!\ ATTENTION CYBER ATTAQUE /!\

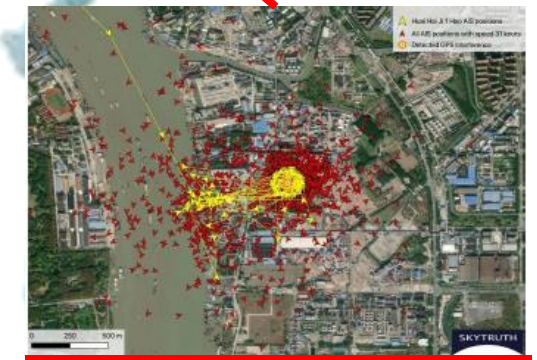
SUITE CYBER ATTAQUE VEUILLEZ NOTER LES ADRESSES DE SECOURS :

- RESPONSABLES D'EXPLOITATION : operations@intramar.fr
- EMPOTAGE / DEPOTAGE / COMMERCIAL / LITIGE : commercial@intramar.fr
- SHIPPLANNING : co@intramar.fr
- GARE / GATE : gare@intramar.fr
- FACTURATION : facturation@intramar.fr
- CONTENTIEUX contentieux@intramar.fr
- COMPTABILITE : compta@intramar.fr
- DAF : sarti.l@marseille-manutention.com
- SERVICE IT : it@intramar.fr
- MAINTENANCE / TECHNIQUE : dt@intramar.fr

Voir toutes les actualités

Mars 2020 – Marseille / FOS - Attaque Région SUD

2020 – Mediterranée (Brouillage GPS)



Jan 2020 – Mer de Chine (Spoofing AIS)

La Maison Cyber du Maritime

Conseil Cyber du Monde Maritime (C2M2)

- COMEX
- C. Analyse des risques
- C. Prospective et régulation

Centre de coordination

- Comité stratégique de pilotage
- Conseil d'administration
- M-ISAC
- Analyser le risque et partager les informations CYBER
- M-SOC
- M – CERT
- EXP / FORM

Surveiller les activités	Détecter les attaques et incidents et les traiter efficacement	Investiguer et collecter les éléments de preuves liées aux incidents et cyber-attaques	Gérer les situations de crise en cas d'incidents majeurs	Améliorer la cybersécurité des systèmes

- Administrations
- Opérateurs portuaires
- Ports
- PME / ETI maritime & offshore
- Opérateurs maritime

La mutualisation – Quels bénéfices ?

Accompagnement des OIV / OSE

Prise en compte des ETI / PME, sources potentielles d'attaques

Bénéfice des projets nationaux et UE (P.I.A 4 / C.S.F / C.E.F)

Outils partagés

- Connaissance et anticipation: THREAT INTEL
- Surveillance des systèmes (PCS / CCS)
- Surveillance des réseaux
- Protection des systèmes spécifiques (AIS / GNSS)

Partage des capacités / couts

- SOC portuaire
- Être la locomotive du maritime
- Ne pas oublier les plus petits