



AAPA 2019

VIRGINIA

REVOLUTIONIZING AMERICA'S FIRST PORT




MPS-ISA0 CASE STUDY EXAMPLES

The Value of Cyber Security Information Sharing to the Maritime Industry

TLP-GREEN



NIST CYBER SECURITY FRAMEWORK

Function	Category	ID 
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO



2015 LEGISLATION TO PROMOTE CYBER SECURITY INFORMATION SHARING

Presidential Executive Order 13691 – Feb. 2015

Promoting Private Sector Cybersecurity Information Sharing

Protecting Public Health & Safety, National and Economic Security

Critical Infrastructure | Sector & Sub-Sector

Business, Industry & Academia | Geographic

Public/Private Collaboration

Cybersecurity Information Sharing Act of 2015....

Signed into law – December 2015

Definitions

Federal Sharing

Protection - Personal Information

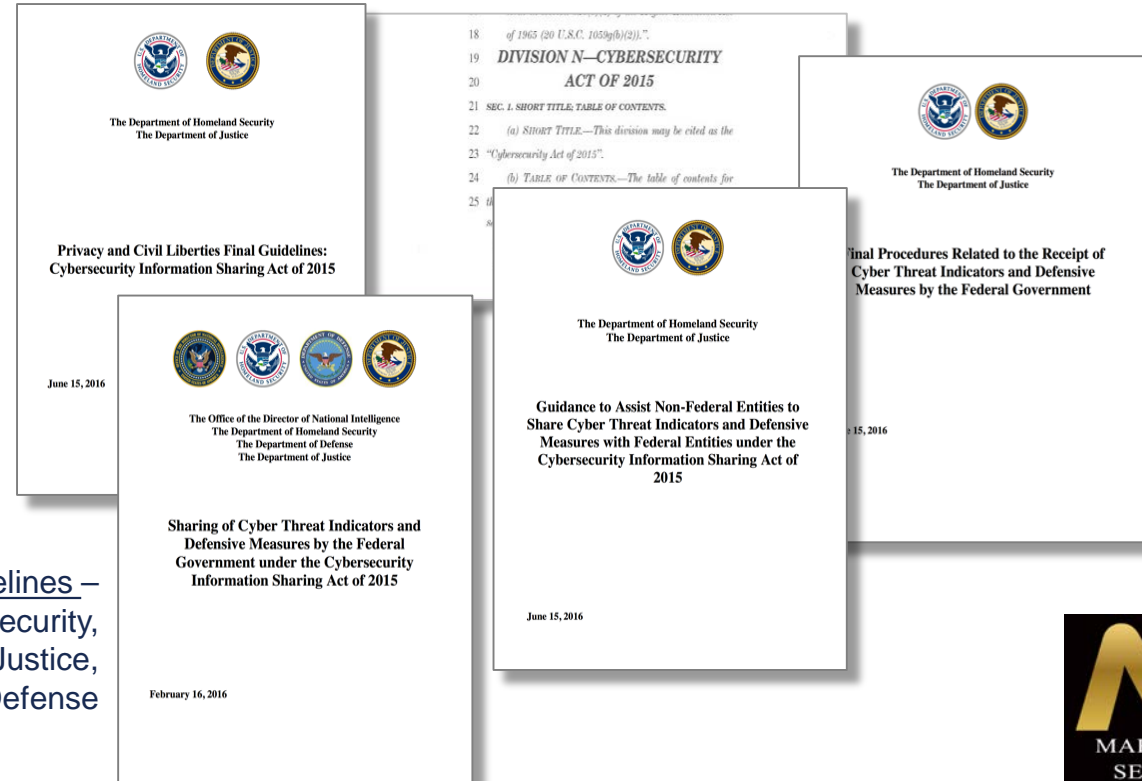
Private Sector Sharing and Liability Protection

Federal Government Published Guidelines –

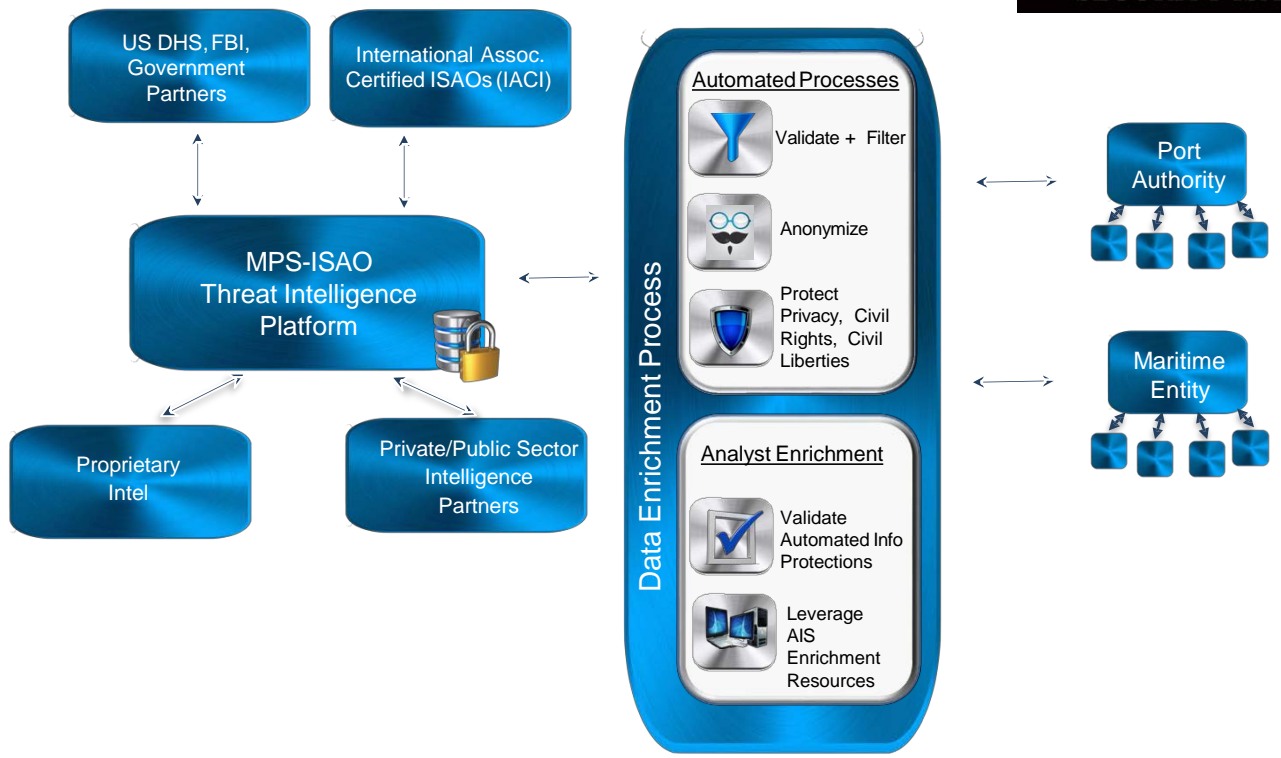
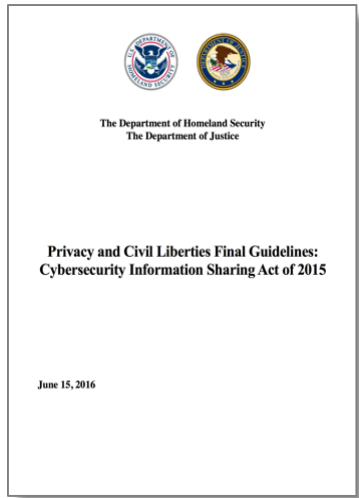
US Dept. Homeland Security,

US Dept. of Justice,

US Dept. of Defense



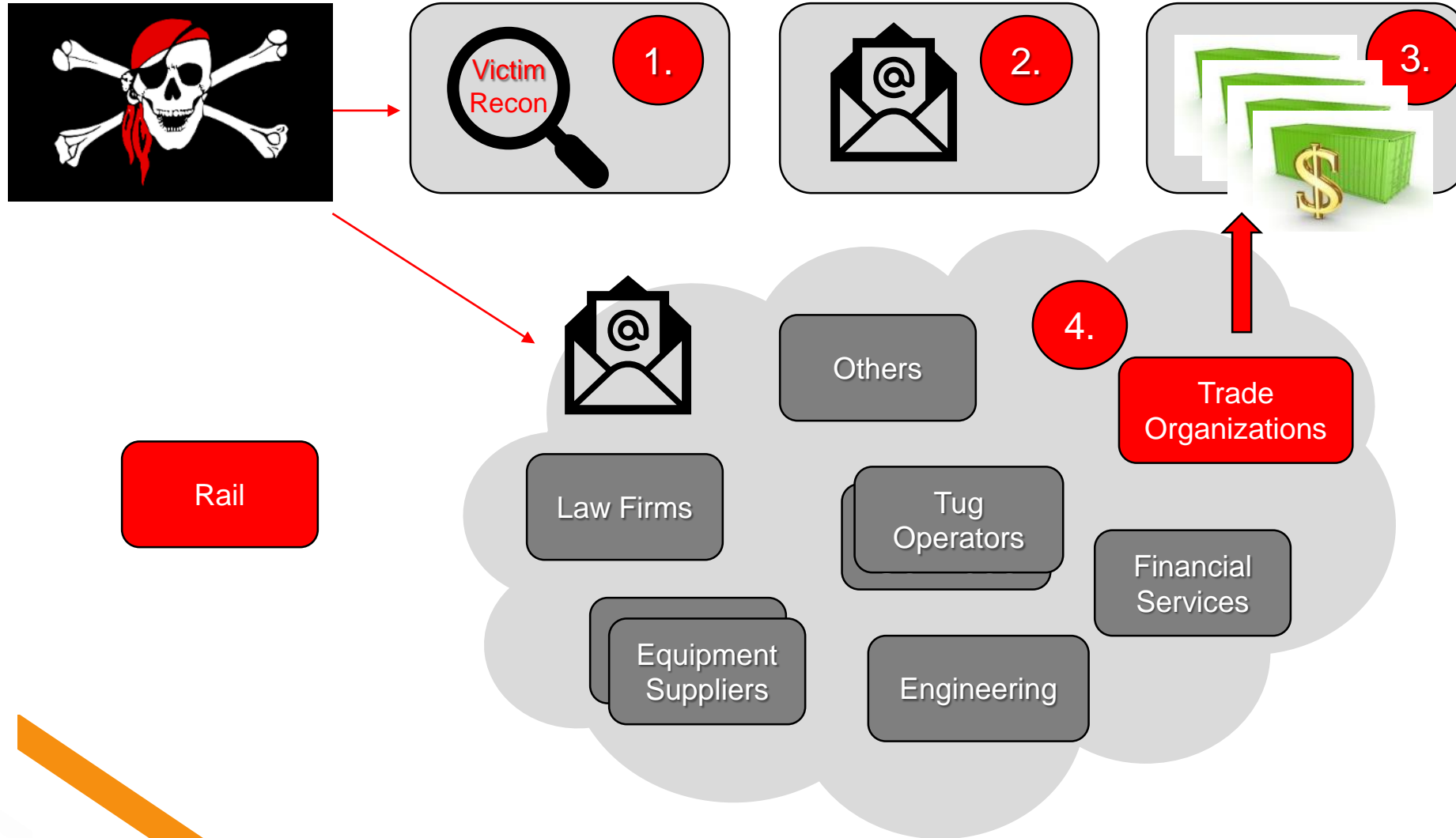
CYBER SECURITY INFORMATION SHARING ECOSYSTEM



Key Ingredients:

- Framework
- Trust Model
- Quality Analytics
- Really Good Intel...
- & CISA

HOW ADVERSARIES TARGET THE MARITIME INDUSTRY?



RANSOMWARE



THE MARITIME & PORT SECURITY
INFORMATION SHARING & ANALYSIS ORGANIZATION

TLP-AMBER
ADVISORY

EMAIL ANALYTIC RESULTS

Industry: Maritime
Report Date: 20181025

Ransomware

Background

On 25-October-2018, an MPS-ISAO U.S.-based Port customer's employee received an email that appeared to be from a legitimate business contact. However, the employee exercised caution before accessing the embedded URL which would have downloaded a malicious zip file. Below are the results of MPS-ISAO analysis, and a list of indicators to block. The MPS-ISAO will promptly load these indicators into Perch Security sensors.

WHY CYBER SECURITY INFORMATION SHARING WORKS?

Case 1: Two Ports receive same malicious email on same day

10/15/2018	Port #1	221.121.XXX.61	commercial@ra...	MV WAF PASSION / Port Agency Appointment
10/15/2018	Port #2	221.121.XXX.61	commercial@ra...	MV WAF PASSION / Port Agency Appointment

Case 2: Two Ports receive same email on different days; same sender and IP as Case 1

10/15/2018	Port #1	221.121.XXX.61	commercial@ra...	MV SHUHA QUEEN II
10/16/2018	Port #2	221.121.XXX.61	commercial@ra...	MV SHUHA QUEEN II

Case 3: Two Ports receive same email 2 weeks apart; same sender and subject - but different sending IP

11/07/2018	Port #1	185.86.XXX.181	cargotrack@ar...	VM Accord, ORDER: TKHA-A88160011B
11/20/2018	Port #2	43.252.XXX.181	cargotrack@ra...	VM Accord, ORDER: TKHA-A88160011B

PATTERNS & TRENDS EMERGE THROUGH SHARED INFORMATION

Email Date	Sending IP	Sending Email	Subject Line
3-Jan-19	50.XXX.XXX.232	John H [REDACTED] com>	REQUEST INFO :: New RFQ for MV YI CHUN 15 (OUR REF.17CF02627)
23-Jan-19	50.XXX.XXX.232	Rabia B [REDACTED] shipping.com>	MV YICHUN - CTM REQUEST FOR PORT DANGJIN OPL, ETA 27th JAN
29-Jan-19	50.XXX.XXX.232	SGLEE [REDACTED] kr>	M/V.Dato Lucky-New Trial Order 2019
19-Feb-19	50.XXX.XXX.232	Kaori M [REDACTED] shipping.com>	PLS CONFIRM : Sales Confirmation JADE PROSPER Your Ref: JPR20180001
4-Mar-19	50.XXX.XXX.232	kmc@ [REDACTED]	Final Request KOREA MARINECRAFT- for vessel MV MEDI OKINAWA
7-Oct-19	50.XXX.XXX.232	Byeour [REDACTED] port@ [REDACTED] marine.com>	Cargo Receipts Revised

UNEXPECTED FINDS



THE MARITIME & PORT SECURITY
INFORMATION SHARING & ANALYSIS ORGANIZATION

TLP-AMBER
ADVISORY

WARNING REPORT

Serial: WR-19-05-01
Report Date: 20190520
Industries: Maritime
Source: MPS-ISAO

Aggressive Russian Scanning Targets U.S. Ports

Background:

Across the past month, multiple U.S. Ports have reported seeing aggressive scanning (rates as high as 200 scans per hour) for sustained periods (several days) from IP Range 81.2[REDACTED]0/24. Even though MPS-ISAO customers have blocked this IP range, the scanning was consistent.

The MPS-ISAO analyzed these IPs, and it was determined that while the IP range geo locates to Germany, it was allocated to Russia on 17-August-2018. MPS-ISAO analysts believe that Germany sold the IP block to Russia.

Details:

Summary

Prefix: 81.2[REDACTED]0/24

Name: DE-IMPULSE-20181015

Description: ERA LLC

Country: Germany (DE)

IP Addresses: 256

Regional Registry: RIPE

Allocation Status: Allocated

Allocation Date: 17th August 2018

Parent Prefix: 81.2[REDACTED]/22

Allocated Country: Russian Federation (RU)

BLENDING MARITIME SHARES WITH OTHERS...

CREATES A MORE COMPLETE PICTURE

	A	B
16	160.XXX.137.163	16-Sep-19 IACI High Confidence IP
17	160.XXX.137.170	16-Sep-19 IACI High Confidence IP
18	160.XXX.137.210	16-Sep-19 IACI High Confidence IP
19	160.XXX.137.218	16-Sep-19 IACI High Confidence IP
20	160.XXX.138.53	16-Sep-19 IACI High Confidence IP
21	160.XXX.138.71	16-Sep-19 IACI High Confidence IP
22	160.XXX.138.163	16-Sep-19 IACI High Confidence IP
23	160.XXX.138.177	16-Sep-19 IACI High Confidence IP
24	160.XXX.138.219	16-Sep-19 IACI High Confidence IP
25	160.XXX.142.19	16-Sep-19 IACI High Confidence IP
26	160.XXX.142.174	24-Sep-19 MPS Customer Email-Email Campaign
27	160.XXX.143.153	16-Sep-19 IACI High Confidence IP
28	160.XXX.147.143	12-Sep-19 MPS Customer Shared IP Blacklist
29	160.XXX.147.161	12-Sep-19 MPS Customer Shared IP Blacklist
30	160.XXX.153.28	12-Sep-19 MPS Customer Shared IP Blacklist
31	160.XXX.154.5	12-Sep-19 MPS Customer Shared IP Blacklist
32	160.XXX.154.7	12-Sep-19 MPS Customer Shared IP Blacklist
33	160.XXX.156.138	12-Sep-19 MPS Customer Shared IP Blacklist
34	160.XXX.197.139	16-Sep-19 IACI High Confidence IP
35	160.XXX.198.164	24-Sep-19 MPS Customer Email-Email Campaign
36	160.XXX.199.186	16-Sep-19 IACI High Confidence IP
37	160.XXX.201.40	16-Sep-19 IACI High Confidence IP
38	160.XXX.202.138	16-Sep-19 IACI High Confidence IP
39	160.XXX.202.170	16-Sep-19 IACI High Confidence IP
40	160.XXX.203.109	16-Sep-19 IACI High Confidence IP
41	160.XXX.247.44	16-Sep-19 IACI High Confidence IP

Actionable
Intelligence =
Blocklist Provided
to MPS-ISAO
Customers to
Alert/Block on
Traffic from this IP
Range

QUESTIONS?

Christy Coffey

VP of Operations, MPS-ISAO

Christy.Coffey@mpsisao.org



AAPA 2019

VIRGINIA

REVOLUTIONIZING AMERICA'S FIRST PORT

