Securing Critical Infrastructure Across the Maritime and Port Community

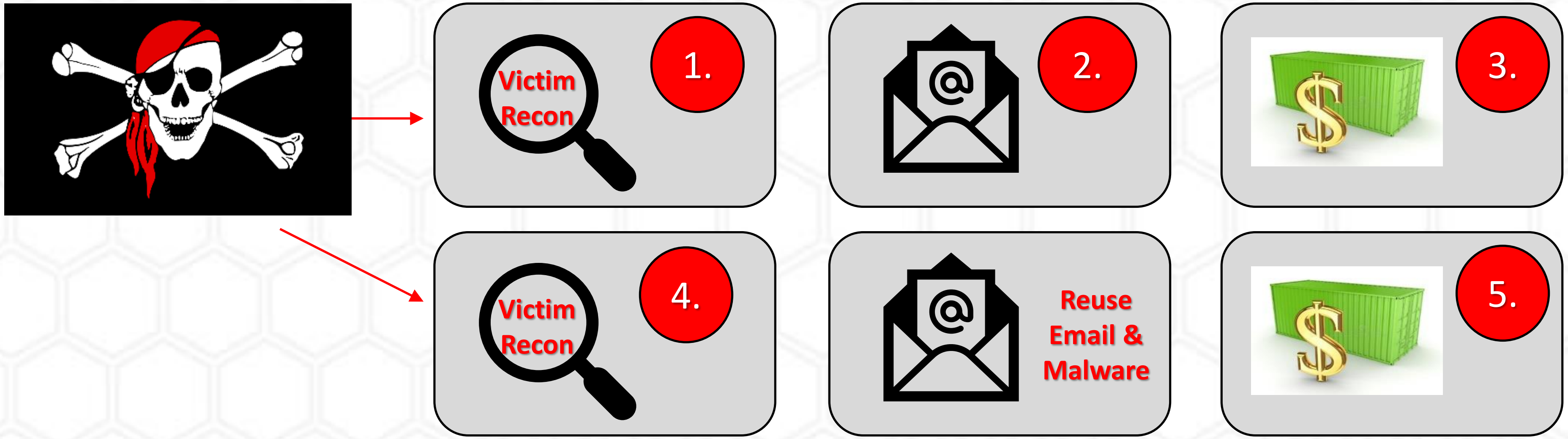
Christy Coffey

VP, Member Services

The Maritime & Port Security ISAO, Inc.

NotPetya

A Case for Working Together



1. Victim Recon

2.

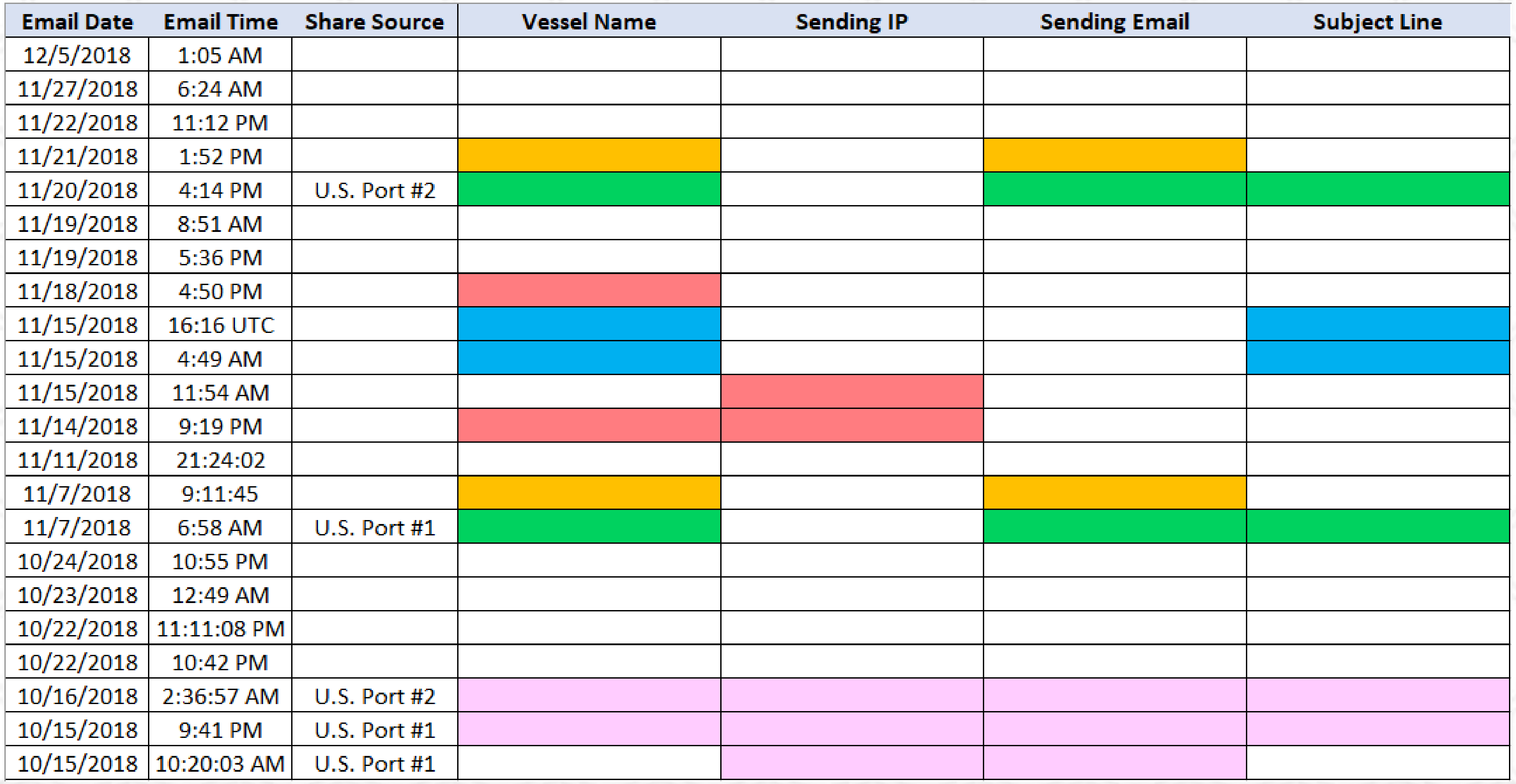
3.

4. Victim Recon

Reuse Email & Malware

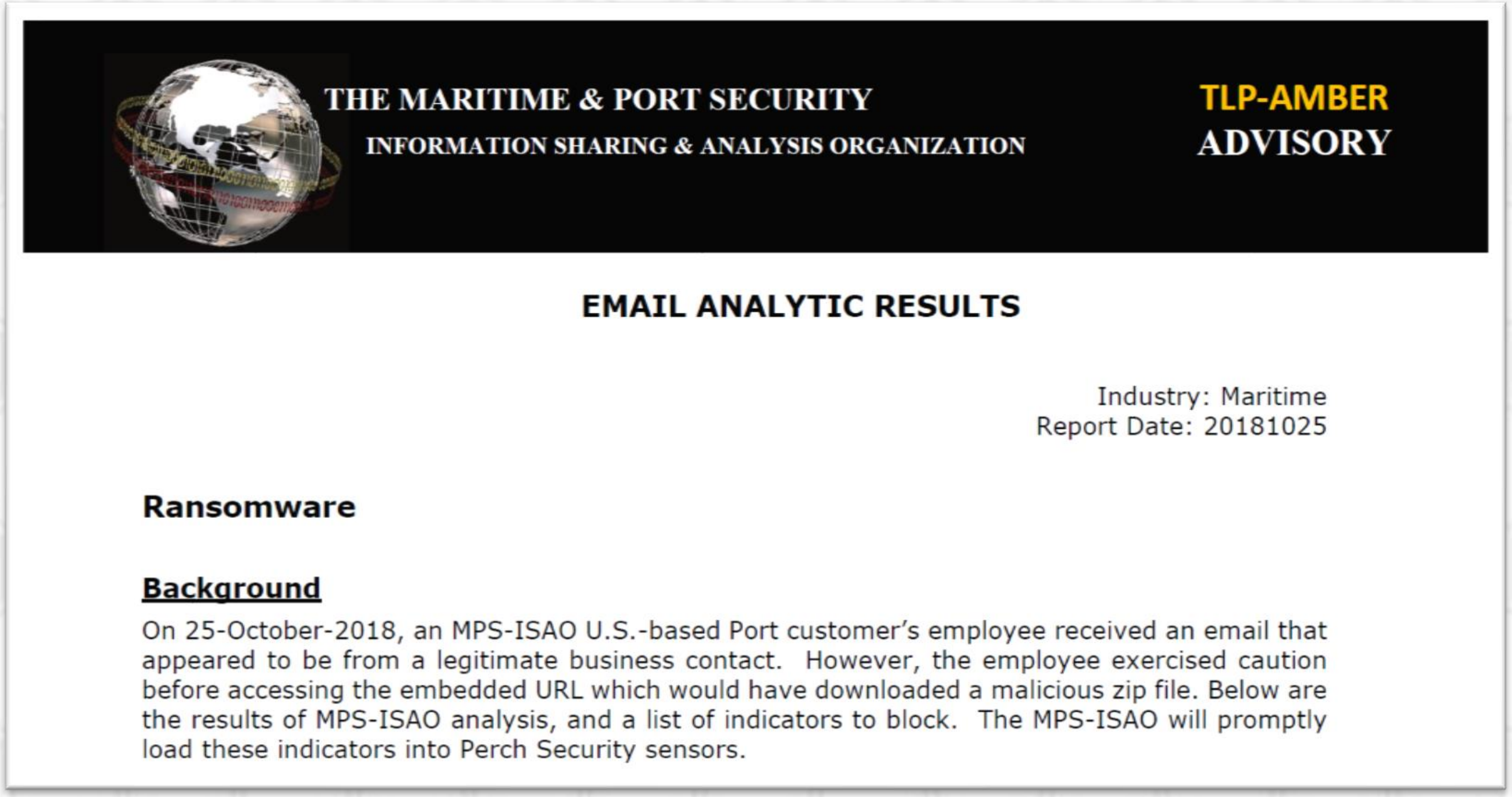
5.

The Proof



Email Date	Email Time	Share Source	Vessel Name	Sending IP	Sending Email	Subject Line
12/5/2018	1:05 AM					
11/27/2018	6:24 AM					
11/22/2018	11:12 PM					
11/21/2018	1:52 PM		🟨		🟨	
11/20/2018	4:14 PM	U.S. Port #2	🟩		🟩	🟩
11/19/2018	8:51 AM					
11/19/2018	5:36 PM					
11/18/2018	4:50 PM		🟥			
11/15/2018	16:16 UTC		🟦			🟦
11/15/2018	4:49 AM		🟦			🟦
11/15/2018	11:54 AM			🟥		
11/14/2018	9:19 PM		🟥	🟥		
11/11/2018	21:24:02					
11/7/2018	9:11:45		🟨		🟨	
11/7/2018	6:58 AM	U.S. Port #1	🟩		🟩	🟩
10/24/2018	10:55 PM					
10/23/2018	12:49 AM					
10/22/2018	11:11:08 PM					
10/22/2018	10:42 PM					
10/16/2018	2:36:57 AM	U.S. Port #2	🟪	🟪	🟪	🟪
10/15/2018	9:41 PM	U.S. Port #1	🟪	🟪	🟪	🟪
10/15/2018	10:20:03 AM	U.S. Port #1		🟪	🟪	

Ransomware



THE MARITIME & PORT SECURITY
INFORMATION SHARING & ANALYSIS ORGANIZATION

TLP-AMBER
ADVISORY

EMAIL ANALYTIC RESULTS

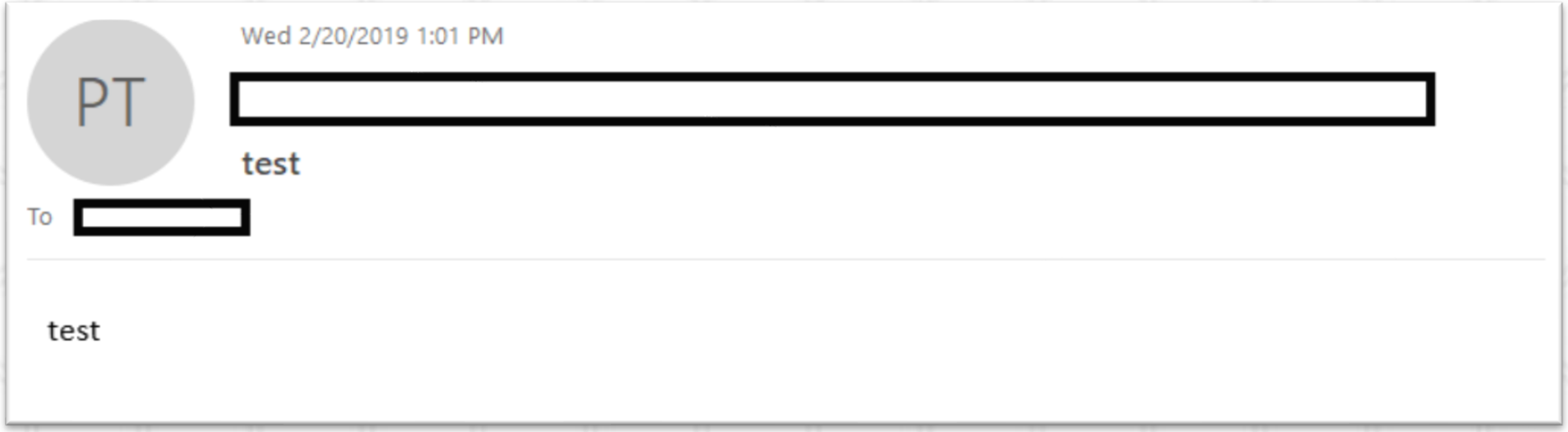
Industry: Maritime
Report Date: 20181025

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.

“Test” Email



PT

Wed 2/20/2019 1:01 PM

[redacted]

test

To [redacted]

test

Christy.Coffey@MPS-ISAO.org

MP

MARITIME & PORT SECURITY ISAO