WARNING REPORT

Serial: WR-19-01-04
Report Date: 20190123
Industries: Maritime
Source: MPS-ISAO

Vessel Impersonation Emails Persist in Maritime Across 2018

Background

In December 2017, the MPS-ISAO issued a Request for Information (RFI) to their customer base to be on the watch for malicious "vessel impersonation" emails targeting their organization. When the MPS-ISAO issued the RFI, the assumption was that adversaries who target one prospective victim using a vessel impersonation email would likely target others by reusing all or part of the email infrastructure. By working together as a community, cyber resilience could be possible. Analysis of the 2018 sample set proved this assumption to be true.

The 2018 RFI resulted in 90 shared malicious vessel impersonation emails. Eighteen different vessel names were used in malicious emails shared by customers to the MPS-ISAO in June 2018 alone. Given the sample set, along with the fact that multiple U.S. ports contributed the emails, the MPS-ISAO was able to identify interesting trends and patterns and demonstrate the importance of community working together. Please note that U.S. Port customers continue to share malicious vessel impersonation emails into 2019 with four reported January 22 thru 23.

About the Threat

Adversaries often use vessel impersonation email to target unsuspecting maritime victims with phishing campaigns or with malware used to harvest credentials for financial theft purposes. Typically, these emails use a legitimate named motor vessel or tanker in the subject line along with a theme that will likely encourage their opening. It is not uncommon for the vessel to have never visited the port. Common subject line themes include "Bunker Request", "Invoice", and "Port Agency Appointment".

Based on 2018 samples received by the MPS-ISAO, some emails include a malicious attachment, while others embed a URL. Anti-virus success blocking these emails has been mixed.

While all samples received by the MPS-ISAO in 2018 were shared by U.S. Port customers, of interest is that the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) shared an Indicator Bulletin (IB) in January 2018 tagged "Financial Services" that included a motor vessel impersonation-themed email subject line. This NCCIC IB provides additional insight in that motor vessel impersonation emails could be targeting the maritime supply chain, including financial services providers, as prospective victims.

The Importance of Community Shares

The graphic below illustrates malicious motor vessel impersonation emails provided to the MPS-ISAO by U.S. port customers during an eight-week period ending December 5th. Data associated with these malicious emails has been redacted and replaced with color coding to illustrate when the vessel name, sending IP, sending email, and/or subject line were re-used between emails directed to U.S. ports.

WARNING REPORT

Email Date	Email Time	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	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	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	Port #2				
10/15/2018	9:41 PM	Port #1				
10/15/2018	10:20:03 AM	Port #2				
10/15/2018	5:24 AM	Port #1				

Figure 1: MPS-ISAO Graphic of U.S. Port Customer Shared Malicious Motor Vessel Impersonation Emails

The purple blocks (bottom two rows) show that on October 15th two U.S. ports received identical emails – matched on full subject line (including motor vessel name), sending email address, and sending IP. However, port one also received a second email on the fifteenth which reused the sending IP and sending email address (purple) but had a different vessel name and subject line (pink). A day later, port two also received the second email (purple/pink blocks). *So, across two days, two U.S. ports, from different geographies and conducting different business operations, saw two identically matched malicious vessel impersonation emails*. The green fill shows that these two ports received similar emails sent almost two weeks apart (November 7th and 20th respectively). Furthermore, red, yellow, and blue fills show where other emails partially matched.

Conclusion

This report highlights that early situational awareness and prevention can be achieved through information sharing. The MPS-ISAO continues to collect malicious email samples, vessel impersonation and other, from customers. These emails are analyzed by the MPS-ISAO's staff of cybersecurity intelligence analysts with the TLP-AMBER results shared with customers.[1]

The MPS-ISAO encourages organizations to monitor their environment for malicious motor vessel impersonation emails, and report sightings to operations@mpsisao.org.
We appreciate the community's support.

End of Report.

[1] https://www.us-cert.gov/tlp

Global Situational Awareness Center – NASA/Kennedy Space Center, FL, operations@mpsisao.org. 904-476-7858

WARNING REPORT

About MPS-ISAO

Headquartered at the Global Situational Awareness Center (GSAC) at NASA/Kennedy Space Center, the MPS-ISAO is private sector-led working in collaboration with government to advance Port and Maritime cyber resilience. The core mission to enable and sustain a safe, secure and resilient Maritime and Port Critical Infrastructure through security situational intelligence, bi-directional information sharing, coordinated response, and best practice adoption supported by role-based education. The MPS-ISAO is a founding member of the International Association of Certified ISAOs (IACI) and is a 2019 CSO50 Honoree. More information at: www.mpsisao.org.