Cyber-MAR Final and Piraeus Pilot Event

Piraeus Pilot Introduction

Giorgos Papavassiliou, ICCS

16th December 2022

Introduction to the Port of Piraeus Container Terminal

- The Port of Piraeus is the first port in the Mediterranean and the fourth port in Europe in terms of container throughput

- It is one of the fastest growing ports worldwide during the last decade handling a wide variety of cargo.

- It is of utmost importance to EU trade and the European economy in total.

Port of Piraeus
Container Terminal

Pilot introduction

- The pilot scenario includes the simulation of a **combined attack** targeting the SCADA system controlling level crossing barriers around the train yard followed by the main attack to the port's network, wiping out the entire IT and OT infrastructure and also causing a cut off to the terminal's power supply
- The attack is structured in 2 Phases:
  - Phase 1 includes a malware execution aiming to steal Security Team Employee's LAN credentials and sensitive information regarding port and railway operations
  - Phase 2 includes the initiation of the combined attack to the port container terminal's IT and OT infrastructure

Pilot Scenario Set-up

- Malware execution through USB key to gain access to the Security Team Employee’s computer
- Sensitive information, such as internal documents regarding port and trains, train timetables, SCADA system documentation and VPN Teamviewer - LAN connection credentials, is stolen
- Attackers profits the access from existing backdoor and gain access to the SCADA system that controls the level crossing barriers at the port’s train yard
- PLCs are reprogrammed to misfunction causing a disruption and eventually a collision between incoming train and trucks
- The incident response process initiated didn’t detect the stolen credentials and the access to the attacked machine was renewed, allowing lateral movement to other machines in the network using TeamViewer and accessing the smart grid’s SCADA system
- Malicious code dropped, and main attack launched wiping out IT and OT infrastructure causing a cut off to the port’s power supply and a consequent major disruption in port’s operations

Pilot objectives

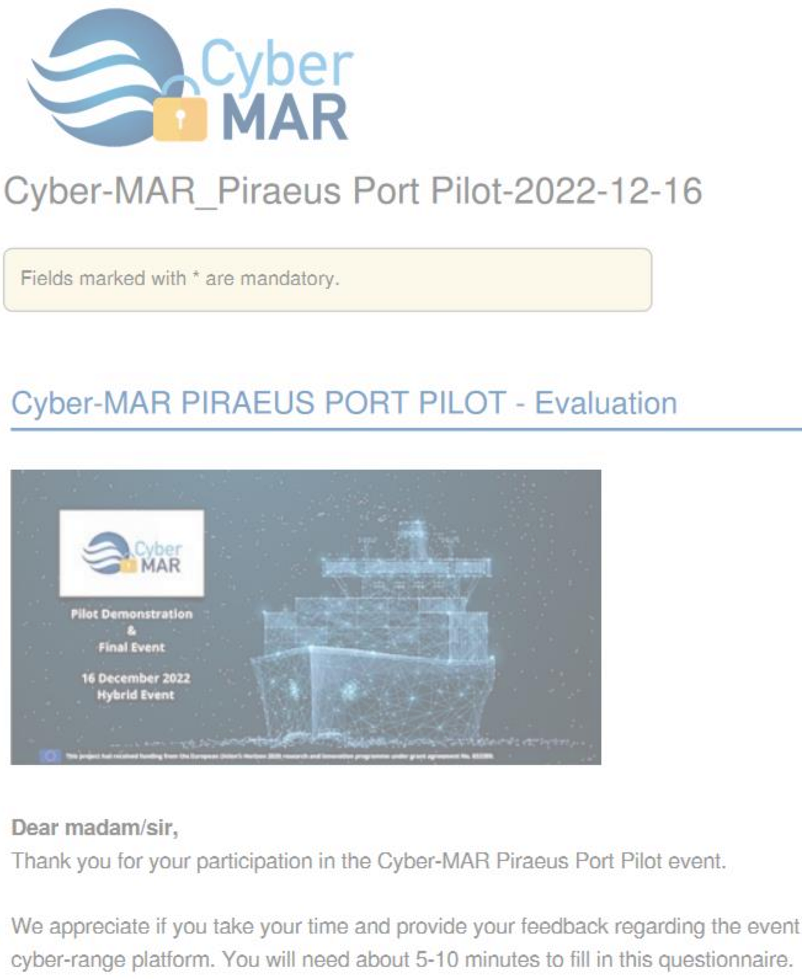
- Assess cyber risk for port's IT and OT infrastructure
- Highlight the consequences and the economic impact of such cyber-attacks to the port terminal's operations
- Increase stakeholders' cybersecurity awareness
- Prepare port personnel to mitigate and restore systems in case of a cyber attack
- Underline the necessity of keeping offline back-ups and spare machines for quick restoring operations
- Test and demonstrate the capabilities of the Cyber-MAR platform and components

Feedback of the Cyber-MAR Pilot platform and the Event

- We have created a feedback survey for this Pilot Event
- Please provide your views of the Cyber-MAR platform and simulation scenario to be presented
- Feedback questionnaire is available online:

https://ec.europa.eu/eusurvey/runner/Cyber-MAR_Pireaus_pilot_16122022

- Answering should take about 5 minutes.
- **Your feedback will help us evaluate the results of our work!!**



Cyber-MAR_Piraeus Port Pilot-2022-12-16

Fields marked with * are mandatory.

Cyber-MAR PIRAEUS PORT PILOT - Evaluation

Dear madam/sir,
Thank you for your participation in the Cyber-MAR Piraeus Port Pilot event.

We appreciate if you take your time and provide your feedback regarding the event cyber-range platform. You will need about 5-10 minutes to fill in this questionnaire.

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Giorgos Papavassiliou, ICCS

✉ giorgos.papavassiliou@iccs.gr

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement No. 833389