Cyber-MAR Valencia pilot

Pilot description

Pablo Giménez, Fundacion Valenciaport

16th December 2020

Scenario introduction

- Scenario is based on the electrical grid communication network of the Valencia port

- There are several systems and equipment deployed throughout the port

- Furthermore, other companies premises are located in the port

- Therefore, power is an essential service to maintain the port activity

- The port authority, as the energy provider within the port, need to protect the infrastructure

Scenario objective

- Assess the electrical grid system to adapt it to avoid any kind of cyber-attack

- Be prepared to mitigate and restore the system in the case of having an attack

- Train port personnel in the necessary skills in cyber threats and quick response in case of emergency

- Test some of the components of the Cyber-MAR components

Scenario architecture

Scenario cyber-attack
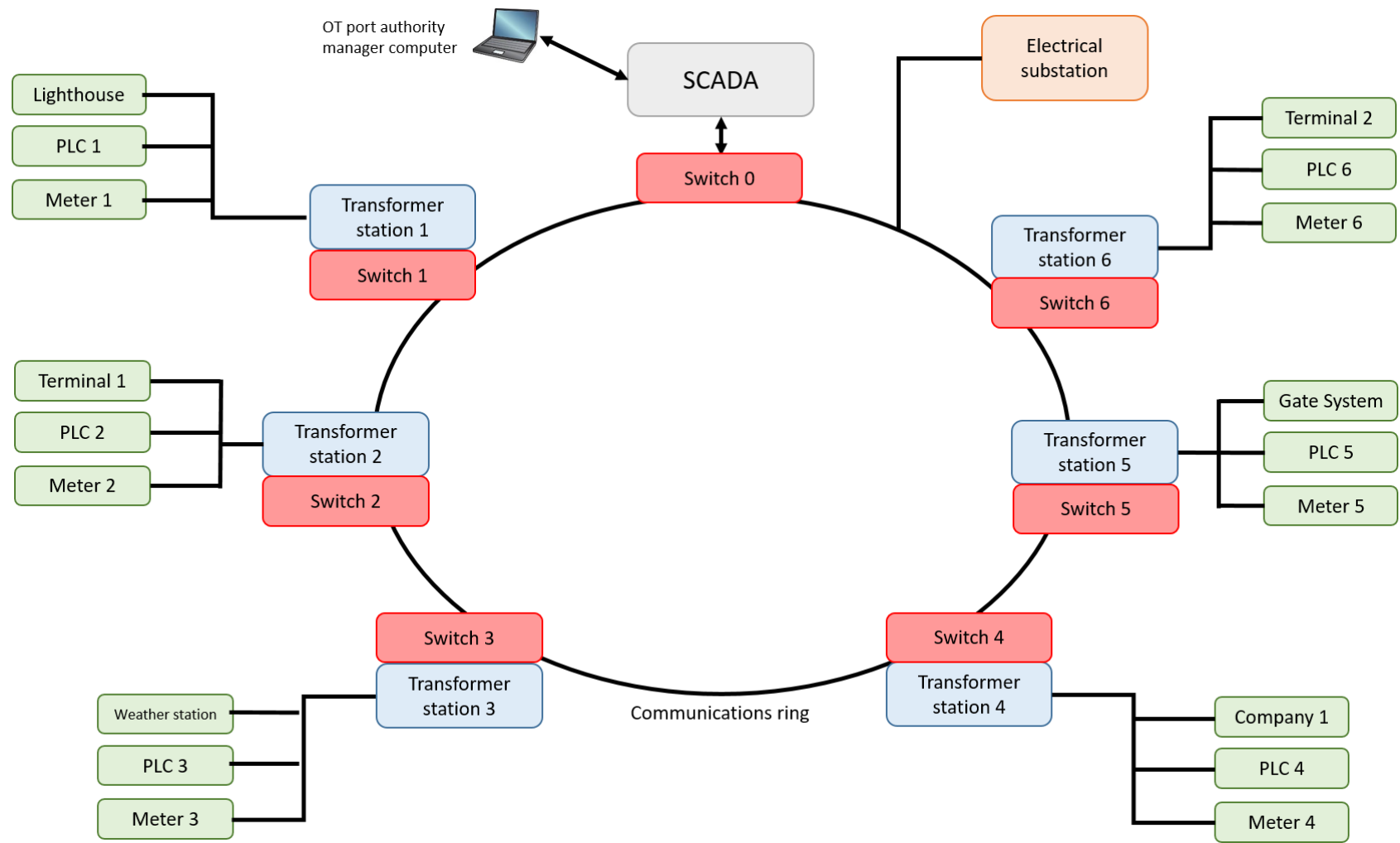
- Cyber-attack to compromise the port electrical infrastructure

  - Phishing email to gain access to the OT manager computer

  - Infect and ransom all the computers in the network

  - Access to SCADA and the PLCs to reprogram them and cut the power

Cyber-attack | Figures & Facts

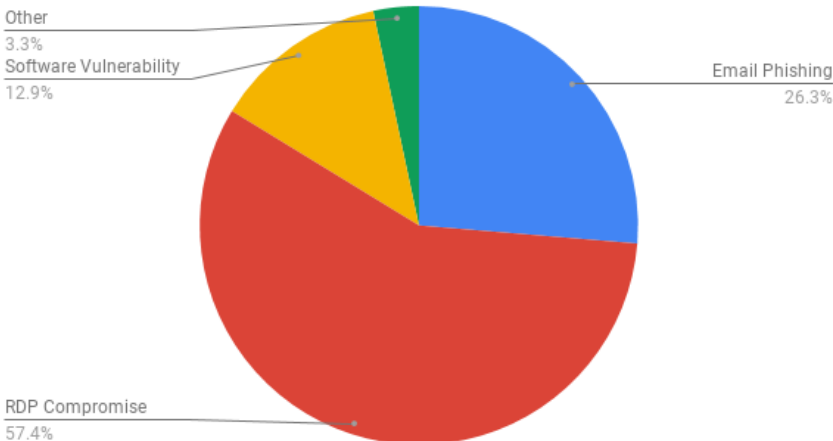## Ransomware Ecosystem

Figures and Facts

How Often Is a Decryption Tool Delivered After Paying a Ransom?

98% Payment Success Rate

Do Ransomware Decryptor's Work?

97% Recovered

3% Lost

Most Common Ransomware Attack Vector Q4 2019

Other
3.3%

Software Vulnerability
12.9%

Email Phishing
26.3%

RDP Compromise
57.4%

What Cryptocurrencies Are Used to Pay for Ransomware?

99% Bitcoin

1% Dash or other privacy coins
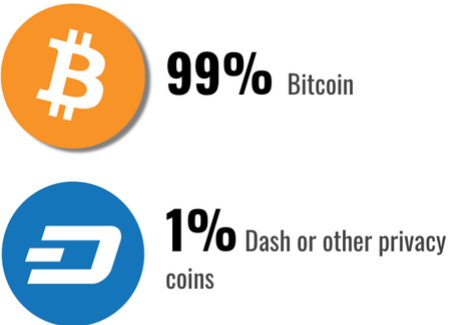
How Much Downtime Does a Ransomware Attack Cause?

16.2 days Average number of days a ransomware incident lasts

Cyber-attack | Figures & Facts
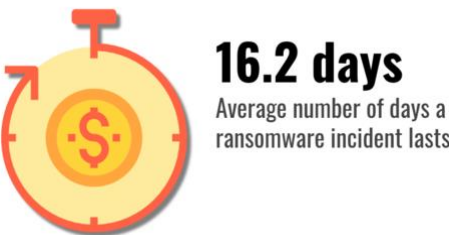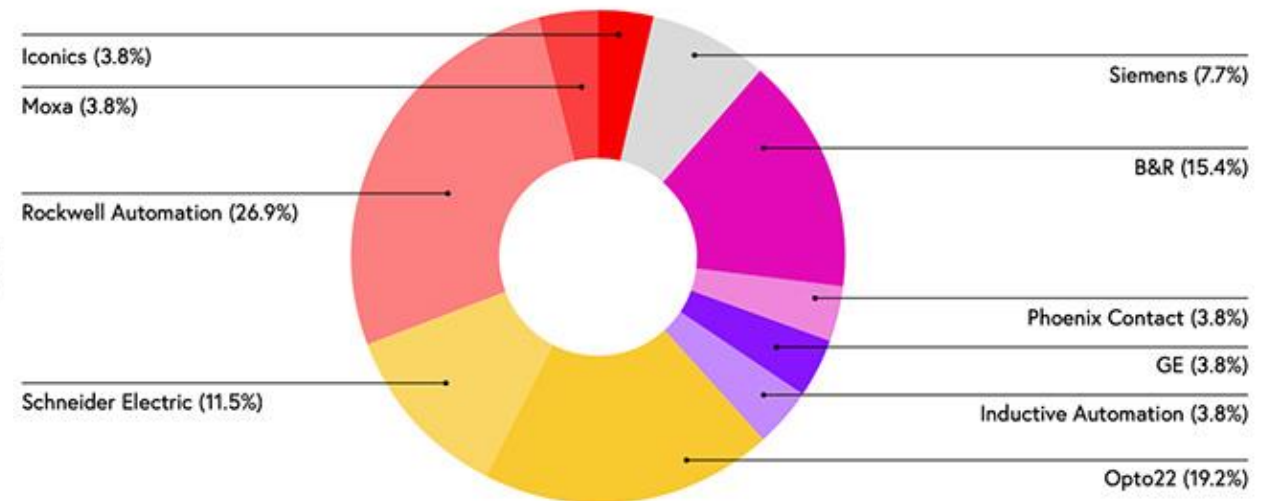
According to the Claroty 2020 report,
+70% of ICS (Industrial Control Systems) vulnerabilities published by the NVD can be exploited remotely

CVSS SEVERITY RATINGS OF NVD-PUBLISHED VULNERABILITIES

Low (1.1%)
Critical (22.47%)
Medium (23.29%)
High (53.15%)

AFFECTED ICS VENDORS

Iconics (3.8%)
Moxa (3.8%)
Rockwell Automation (26.9%)
Schneider Electric (11.5%)
Siemens (7.7%)
B&R (15.4%)
Phoenix Contact (3.8%)
GE (3.8%)
Inductive Automation (3.8%)
Opto22 (19.2%)
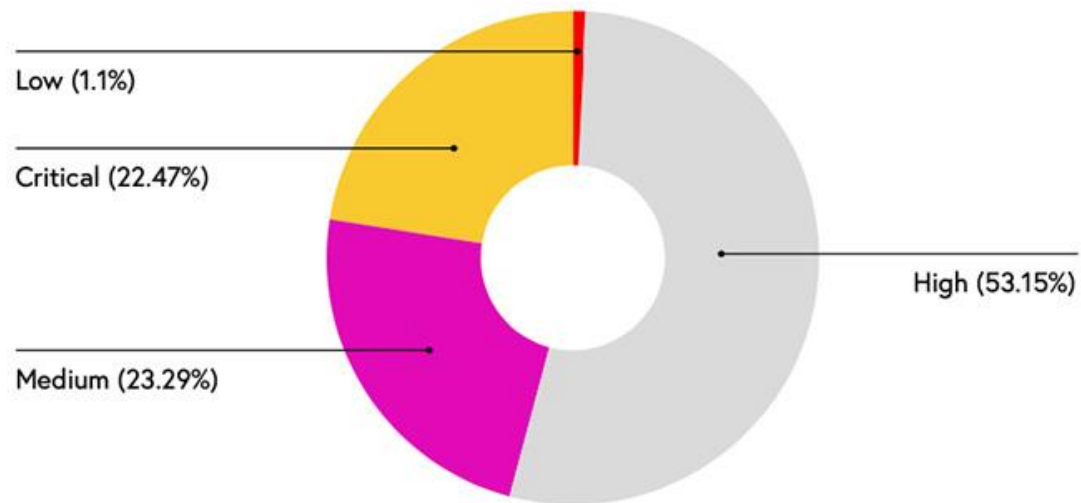
Conclusions

- Importance of cyber-security

- Big economic impact on a port infrastructure

  - Severe incident could need from hours to days to recover

- Cyber-range added value

  - Test all kind of vulnerabilities in your systems

  - Training for all the company personnel

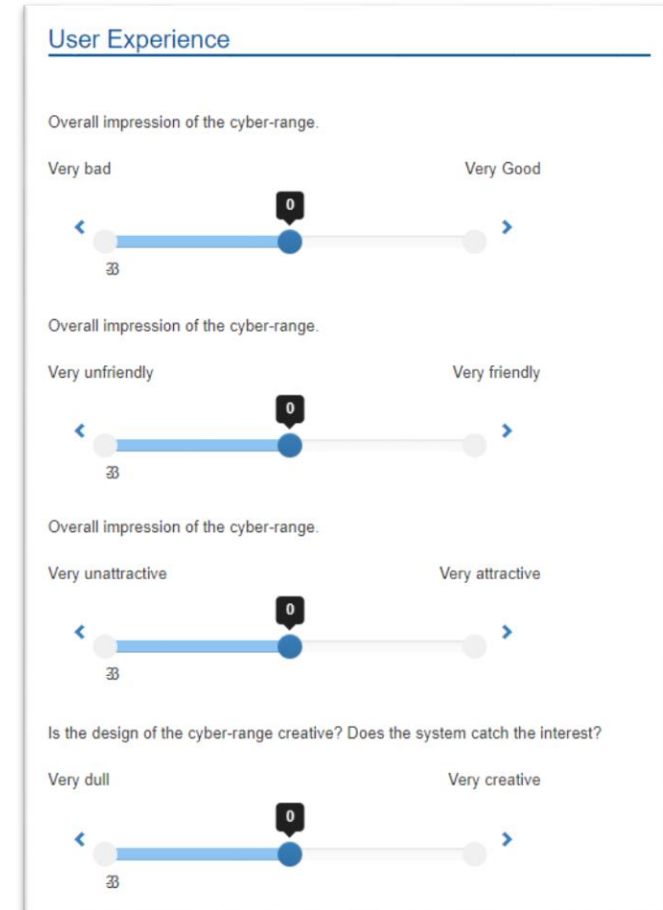# Feedback of the Cyber-MAR Pilot platform and the Event

Feedback needed and valued for

- Cyber-MAR platform and cyber-ranges' development

- Further pilot events planning

Feedback questionnaire is online: (*link available in chat and email)

https://ec.europa.eu/eusurvey/runner/Cyber-MAR_Valencia-Pilot-2020

- Answering should take about 5 minutes.

- **Your support will help Cyber-MAR to improve and better serve your needs!**

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION