Situational awareness: known cybersecurity incidents targeting ports

HudsonCyber
Managing Cyber Risk

Chronis Kapalidis, Hudson Cyber, Hudson Trident UK

About Us

"Global maritime transportation systems are evolving rapidly as technology and advanced analytics drive innovation and challenge existing approaches to risk management. The art of the possible is changing. We must change with it." ***ADM Thad Allen (USCG Ret.)***

HudsonAnalytix
Complexity made simple.

Leading Edge Maritime Risk Management

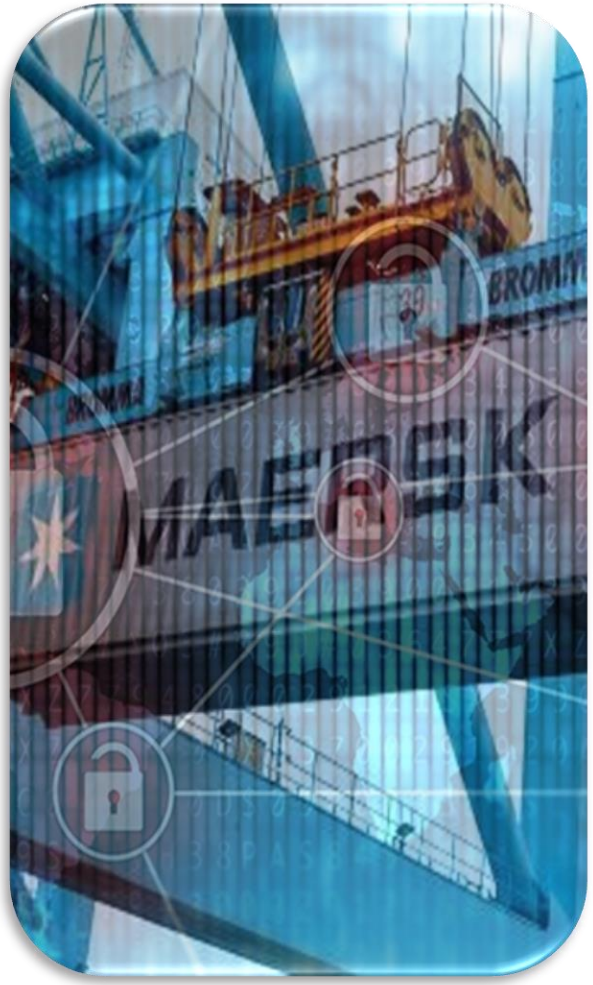
tel: +1.856.342.7500
www.hudsonanalytix.com

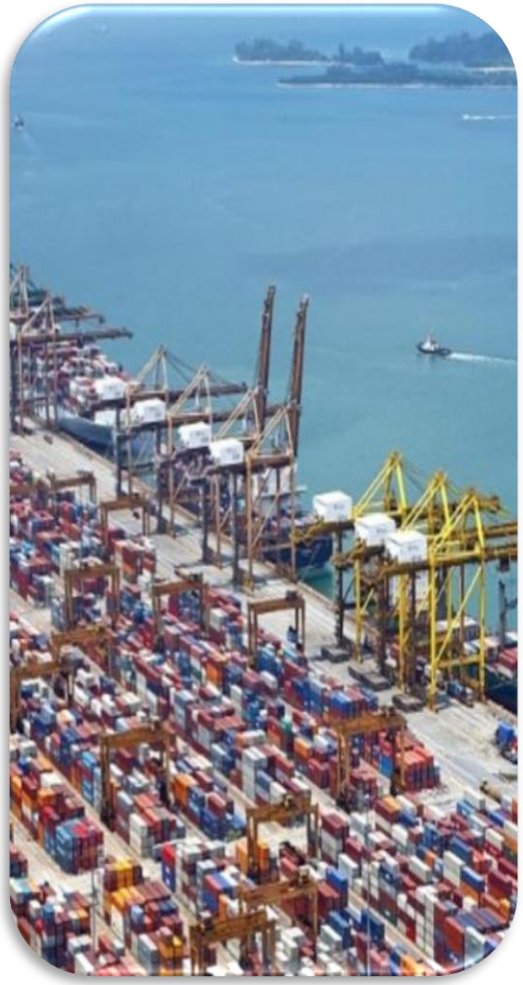
Key Facts

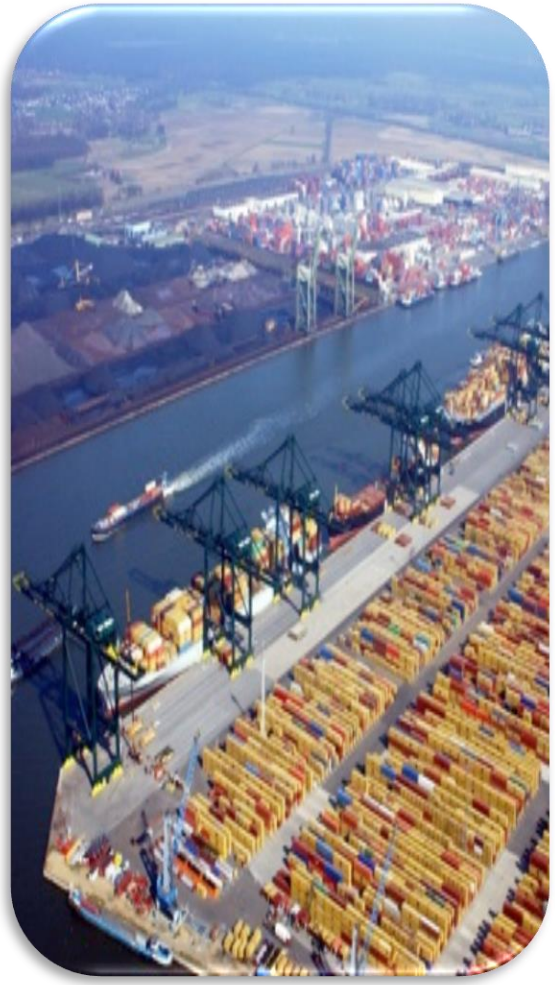
- Founded in 1986
- Worldwide Presence:
  - Philadelphia (Global HQ)
  - Washington, DC
  - San Diego, CA
  - London, UK
  - Rome, Italy
  - Piraeus, Greece
  - Manila, Philippines
- Industry Leaders in Maritime Risk Management Solutions and Support Services

Partners CIP Inter-American Committee on Ports | NTELOX Insight to Action | AON Empower Results® | DNV·GL

Case Study Analysis







CASE STUDY I: MAERSK - NOTPETYA

NotPetya Malware Attack: Timeline

Company's helpdesk in India

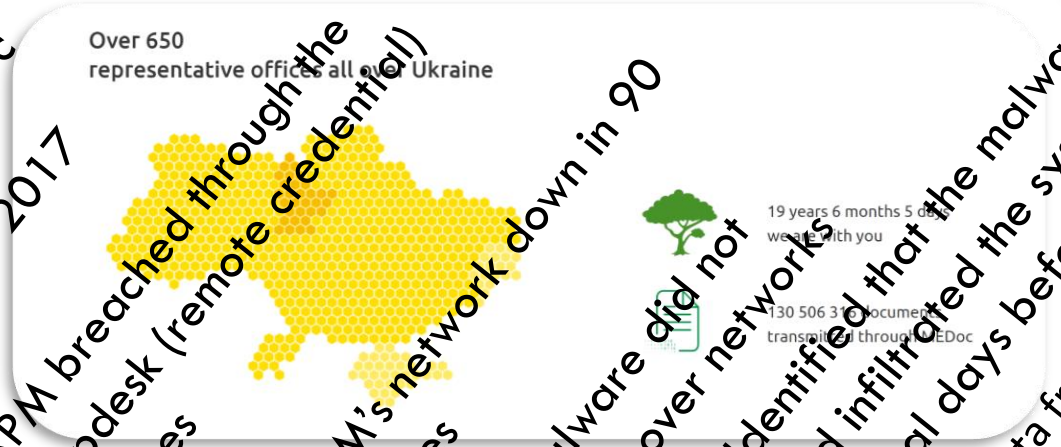
2014 Development of cyber strategy

Pen Testing. Poster based maritime cyber awareness programme

NotPetya Anatomy: 4 methods of propagation – Targeted MeDoc

1530 EET 27 June 2017

APM breached through the helpdesk (remote credential) services



APM's network down in 90 minutes

Malware did not jump over networks

Identified that the malware had infiltrated the system several days before the attack

EDI data from ships was wiped

WHY?

Underinvestment in IT infrastructure

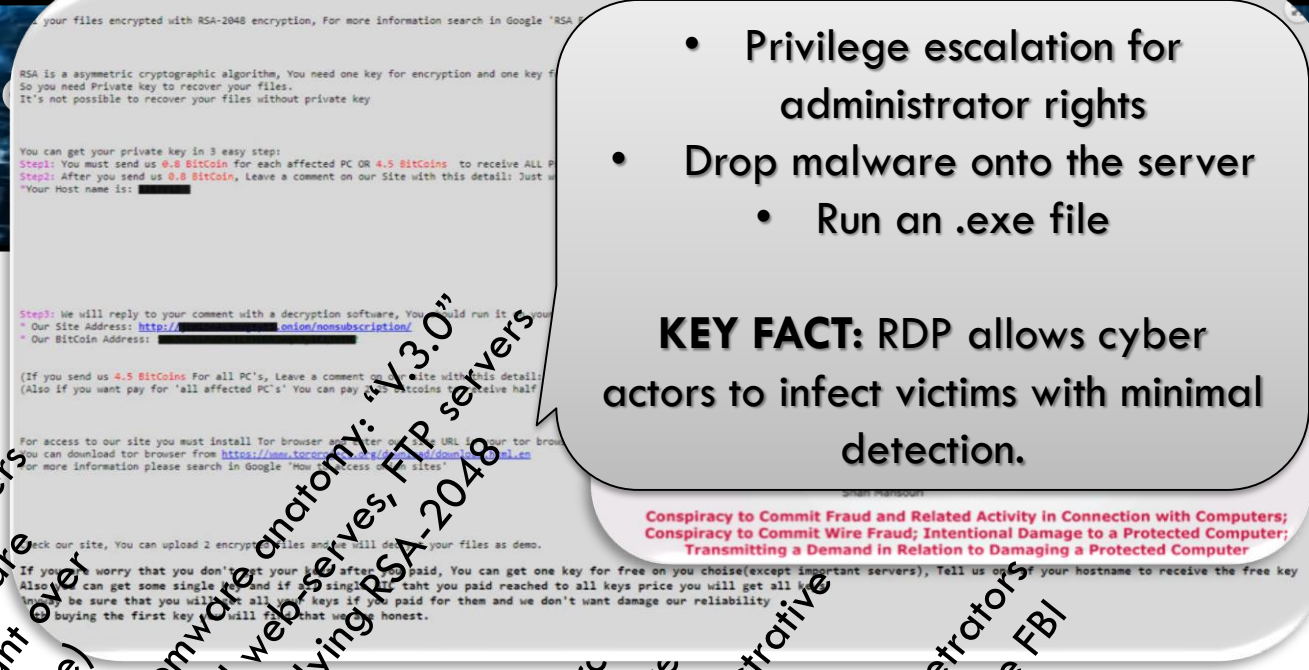
Background/Reconnaissance/Weaponization

Attack/Delivery

Recovery/Forensics

CASE STUDY II: PORT OF SAN DIEGO

State-Sponsored Ransomware Attack Timeline



- Privilege escalation for administrator rights
- Drop malware onto the server
- Run an .exe file

KEY FACT: RDP allows cyber actors to infect victims with minimal detection.

One case within a coordinated ransomware campaign from Dec 2015

25 October 2018

Iranian state-sponsored hackers launch SamSam ransomware (Bitcoin payments sought over a Tor hidden service site)

SamSam ransomware anatomy: "V3.0" RDP, Java-based web-serves, FTP servers or Brute force applying RSA-2048 encryption

RDP credentials purc
DarkWeb marketplace
Stole mostly administrative data; not operational

2 months later perpetrators where identified by the FBI

Background/Reconnaissance/Weaponization

Attack/Delivery

Recovery/Forensics

State-Sponsored Ransomware Attack: Timeline

- **September 25, 2018 – Employee files locked and ransom demanded.** All staff directed to shut down computers. Port notifies: Governor and County Offices of Emergency Services, US Coast Guard, US Navy, US Dept. of Homeland Security and FBI.
- **September 26 – Port issues public announcement.** Port mobilizes team of industry experts and government partners to respond to and recover from incident. Police use alternate systems to support public safety. **Staff have limited functionality.** Backup / alternate systems employed.
- **September 27 – Port remains open.** Port issues follow up statements and continues to work with investigators.
- **September 28 –** Cruise ship arrives in port. **All passengers successfully processed.** No delays.
- **October 2 –** Port operations continue normally, but **administrative activities remain impacted.** Alternate systems utilized where possible.
- **October 3 – Payroll successfully processed using alternative system.**
- **October 4 – All operations continue.** Cruise and cargo ships managed with out delays.
- **November 28 –** US Government announces indictments against hackers.

Initial Stage

Recovery process/ media handling

Contingency planning

Recovery/Forensics

CASE STUDY III: PORT OF ANTWERP

A case on the convergence of cyber and physical attack methods

From 2011 to 2013 drug traffickers used hackers to facilitate drug trafficking

Aim was to access secure data, on the location and security details of drug-laden containers arriving at port

Phishing attack with malicious software offering access to port cargo management system

After initial discovery hackers gained physical access and installed key-logging devices

A different mean to the same end

The issue re-emerged in 2018

THE WALL STREET JOURNAL.

English Edition | November 21, 2019 | Print Edition | Video

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

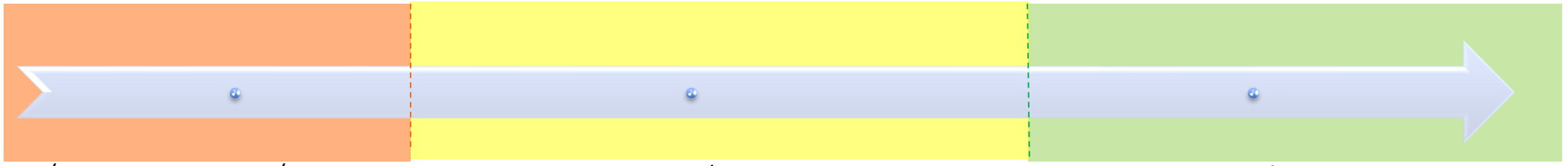
WORLD | EUROPE

Cocaine's New Gateway to Europe: Busy Belgian Port

More of the drug is coming through Antwerp's port as output from Latin America rises

By Valentina Pop

March 1, 2018 7:46 am ET



Background/Reconnaissance/Weaponization

Attack/Delivery

Recovery/Forensics

Case Study Conclusion

Collateral Damage of a state-sponsored APT attack

Value of contingency planning

Motivation: Business interruption

APT attack

Value of business continuity and successful forensic analysis

Motivation: Financial / Business interruption???

APT attack

Highlights the convergence of cyber-physical attack methods

Motivation: Financial

东康公路
行南公路
浦东北路
嘉安路
黄浦江

Thank You

HudsonCyber
Managing Cyber Risk

"If cybercrime was a country,
it would have the 13th highest GDP in the world"