TICTAC
LABORATORIES
CYBER SECURITY • DATA RECOVERY
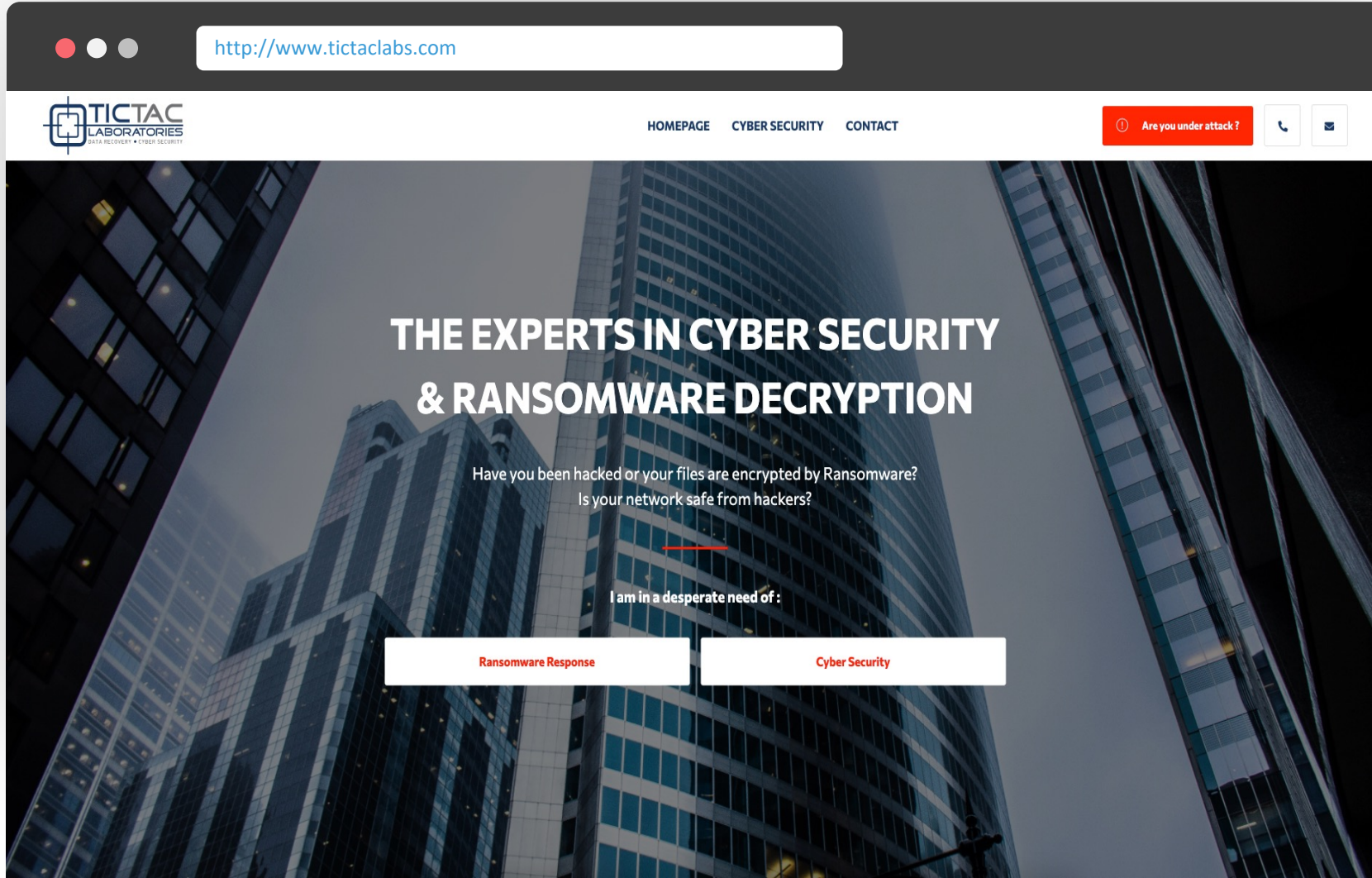
Mitigate
Your Maritime
Cyber Security Risks

OPELLA

ISO 27001 — Information Security Management System Certified
ISO 9001:2008 — CERTIFIED COMPANY

TICTAC CYBER SECURITY

http://www.tictaclabs.com

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

HOMEPAGE   CYBER SECURITY   CONTACT

⚠ Are you under attack ?

THE EXPERTS IN CYBER SECURITY & RANSOMWARE DECRYPTION

Have you been hacked or your files are encrypted by Ransomware?
Is your network safe from hackers?

I am in a desperate need of :

Ransomware Response   Cyber Security

Distributors for Greece & Cyprus for the following products:

COMODO CYBERSECURITY   SecurityScorecard

deepinstinct — BEFORE YOU KNOW IT   Digimune — powered by ZeroFOX

iTARIAN

Resellers & Integrators for the following products:

Acronis | Platinum Partner   CyFIR

Microsoft Silver Partner   pfsense

SHIPS ARE HACKED TOO

It's not a matter of IF

It's a matter of WHEN

All four of the world's largest shipping companies have now been hit by cyber-attacks
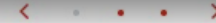
Maritime industry needs to focus more ~~~~~ attacks.

One ship is hacked every day on average

Ships and shipping companies are regularly targeted by cyber criminals, webinar discussion hears

Written by **Catalin Cimpanu**, Contributor
Posted in Zero Day on September 29, 2020 | Topic: Security

With today's news that French shipping giant CMA CGM has been hit by a ransomware attack, this now means that all of the four biggest maritime shipping companies in the world have been hit by cyber-attacks in the past four years, since 2017.

Previous incidents included:

1. APM-Maersk - taken down for weeks by the NotPetya ransomware/wiper in 2017.
2. Mediterranean Shipping Company - hit in April 2020 by an unnamed malware strain that brought down its data center for days.
3. COSCO - brought down for weeks by ransomware in July 2018.

Are You Really Covered?

TICTAC LABORATORIES
CYBER SECURITY • DATA RECOVERY

Managed Backup & Disaster Recovery

30 RANSOMWARE ATTACKS

IN GREEK MARITIME COMPANIES

1 **Targeted attacks in the Maritime Industry**

Hackers have Access to Financial Statements

Ransom Demands is adjusted to company size

2 **Old Fashioned backup processes**

No Cloud Backups

No Disaster Recovery Planning

3 **Multiple ransomware encryption**

Multiple hacker groups may perform a cyber attack at the same time

30 RANSOMWARE ATTACKS

IN GREEK MARITIME COMPANIES

4 Computer Forensics identifies the following:

- 2 months-long unnoticed APTs (Advanced Persistent Threats)

- Encryption took place after corrupting the offline backup files

- Attacker had root access with ability to disable defense mechanisms

5 IT Admins and the central management often perform mistakes during the process of a cyber attack that may render their data being corrupt forever, even after paying the hacker

6 **Numerous cases of Business Email Compromise** SCAM (BEC SCAM)

Our experience in Greek Shipping Cyber-exposure revealed:

1 **Unmanaged endpoint protection** (antivirus) & Firewall
Human oversight is required for effective defense

2 **No Cloud Backup, lack of Disaster Recovery Plan** &
Incident Response Plan & Runbooks
No Anti-ransomware / Big actual downtime

3 **No Active Directory present in many instances** /
lack of Audit trails and system logging

4 **Absence of Logging for third party providers**
with system access

Our experience in Greek Shipping Cyber-exposure revealed:

5   **Unpatched systems, outdated Operating Systems** and non-verified Third-Party applications

6   **Lack of network segmentation and MFA** as per IMO/NIST Guiding principles

7   **Inadequate personnel cybersecurity training** and lack of Cyber Insurance as per IMO/NIST Guiding principles

8   **Lack of Risk Assessment and monitoring** as per IMO/NIST Guiding principles

What Does Ransomware Cost Greek Maritime Companies?

- Your valuable files are lost

- **No communication with ships**

- Financial **losses** from **day one**

- **Legal implications** from data leakage

- Third-party exposure

- No incident response mechanism in place = **nightmare!**

- You cannot see the enemy without special tools

Disaster Recovery & Cyber Security Services for Maritime

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Tictac Cyber Security has created a new all-in-one solution in order to assure that your data is always there when you need it

Your Data is Always Available

24/7

We Protect your Critical Data:

- ✓ Anti-Ransomware Cloud Backup
- ✓ Disaster recovery on the cloud
- ✓ Local Backup if needed
- ✓ Daily Backup monitoring
- ✓ Disaster Recovery Testing

Protect your Infrastructure from Cyber Attacks

We Protect your company from Cyber Attacks

- ✓ Endpoint detection & Response EDR
- ✓ 24/7 Security operation center (SOC)
- ✓ Full monitoring & reporting
- ✓ Remote Management & Monitoring Tool
- ✓ Asset Inventory
- ✓ All-in-One tool / Web Console
- ✓ IMO Cyber Security Compliance

Backup & Disaster Recovery Services

Provided Services & SLAs

- ✓ We guarantee your data availability in case of hardware/software failure or Cyber Attack

- ✓ We guarantee your system restoration in less than 30 minutes with the Disaster Recovery Service

- ✓ We provide Data Storage in Data Centers all over the world, depending on clients' compliance

Your Data is Always Available

We Protect your Critical Data:

- ✓ Anti-Ransomware Cloud Backup
- ✓ Disaster recovery on the cloud
- ✓ Local Backup if needed
- ✓ Daily Backup monitoring
- ✓ Disaster Recovery Testing

24/7

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Managed Cyber Security Services (MSSP)

Provided Services & SLAs

- ✓ Protection from data breach and data exfiltration

- ✓ Advanced Logging of abnormal activities

- ✓ Continuous process monitoring

Protect your Infrastructure from Cyber Attacks

We Protect your company from Cyber Attacks

- ✓ Endpoint detection & response (EDR)
- ✓ 24/7 Security operation center (SOC)
- ✓ Full monitoring & reporting
- ✓ Remote Management & Monitoring Tool
- ✓ Asset Inventory
- ✓ All-in-One tool / Web Console
- ✓ IMO Cyber Security Compliance

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

TICTAC LABORATORIES
CYBER SECURITY • DATA RECOVERY

RANSOMWARE

You need a
Ransomware
Incident Response
Mechanism in place

MSSP Model

1 Endpoint protection (EDR)

Comodo Advanced Endpoint protection offers an EDR solution with auto-cointainment patent pending technology that implements Zer-Trust policy

2 Cloud Managed Backup & Disaster Recovery

Acronis Award wining Ransomware-proof Automated Backup & Disaster Recovery to Cloud along with Disaster Recover Planning

3 Firewall Installation and continuous monitoring

24/7/365 Firewall monitoring service. Extra services include Breach Simulation, Continuous Network Vulnerability Assessment with automated tools

MSSP Model

4 Security Operations Center (SOC)

24/7/365 security monitoring and remediation from human experts. **We don't only observe, we take action**

5 Live Digital Forensics

Using **Advanced Digital Forensics** tools our team perform real time digital forensics and investigate

6 Cyber Insurance

Tictac Cyber Security is the first MSSP provider in Greece that offers a special insurance coverage on top of its services

7 Cyber Security Awareness Training

Cyber Security is about **People**, Tools and Processes. We train the personnel to become **Human Firewalls**

TICTAC
LABORATORIES
CYBER SECURITY • DATA RECOVERY

We safeguard your
Marine Assets

Tictac Cyber Security

Tripoleos 9, Ymittos, Greece

Tel. 2106897383

info@tictac.gr

www.tictaclabs.com