



**DIGITAL TRANSFORMATION**& INDUSTRIAL CYBERSECURITY
IN THE OIL&GAS INDUSTRY



JUNE, 24 & 25 Rio de Janeiro, Brazil

#### **Anatomy of a Cyberattack**

Alexánder Fonseca Moya

Chief Information Officer

# (HRISTMAS) IS AROUND THE CORNER

## **Attacker/Victim profile**

RaaS

Works with affiliates

600 victims worldwide

Sectors: health, government and critical infrastructure

90/10 distribution: affiliates/organization

Revenue by volume

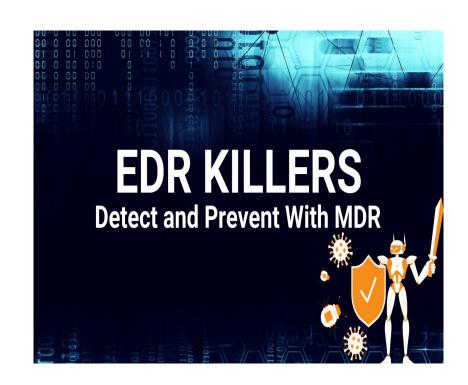
Russia, Cuba, North Korea and China.

Average victim revenue \$390 million

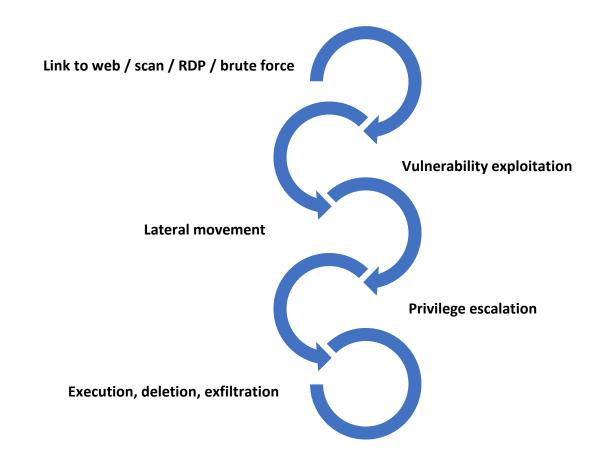
There is a "de-encryption" guarantee

Most dangerous and fastest growing group

**Sophisticated EDR evasion techniques** 



## How did it happen? Phishing?





## ¿What was the impact?

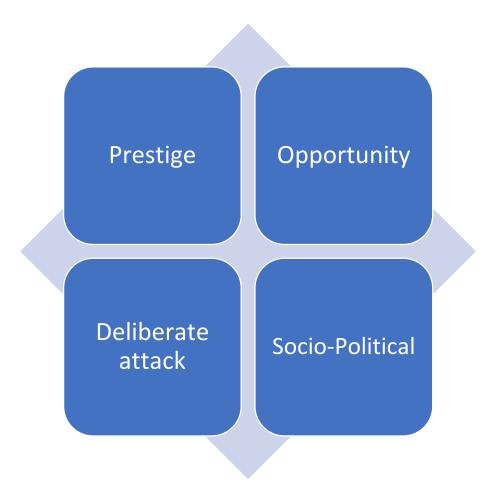
#### Affected

- IT network
- Commercial systems
- Servers
- Systems

#### Not affected:

• End Points

#### ¿Why were we attacked?



#### First minutes...

#### Containment

Turn off Internet

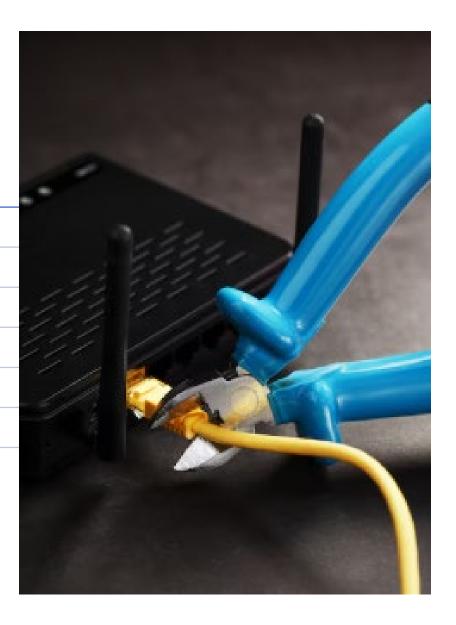
Hijack computers

Activate protocols

Contingency

Turn off equipment \*

Inform the authorities



## Early hours...





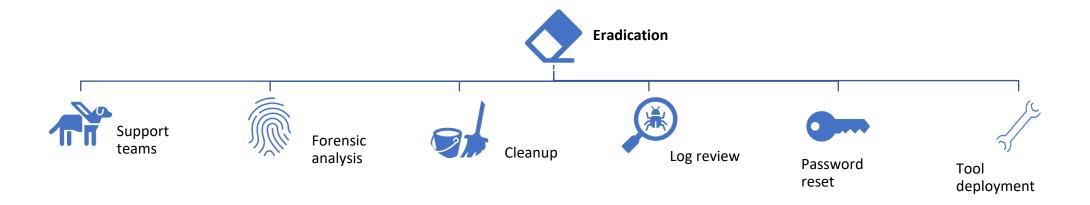


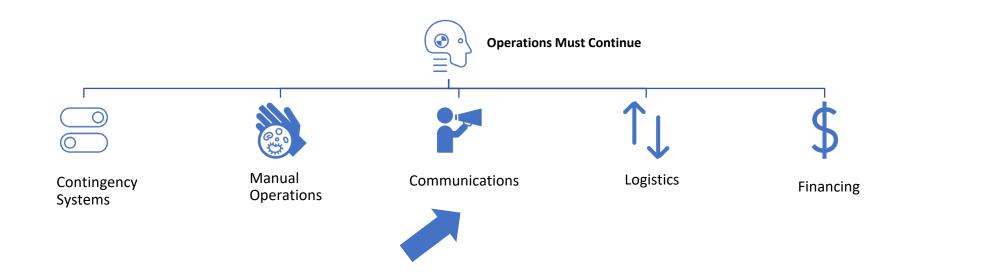


## First Days...





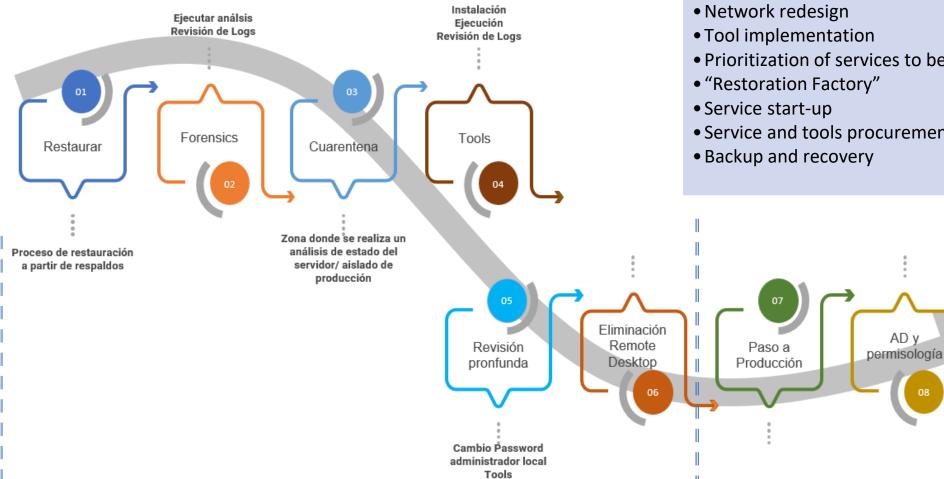




#### **First Months**

#### Recovery

- Recovery Plan
- Basic inputs (infrastructure and backups)
- Prioritization of services to be recovered
- Service and tools procurement



Development

Production

#### **Lessons Learned**

Keep Calm

Education

Monitoring

Visibility

Multi-Factor Authentication

Tools, Al

**USB Lock** 

State Art

Local keys

Backup Strategy

**Credential Vault** 

Magnetic Tape



#### **Lessons Learned**

Physical and logical segmentation

Information Security Management System

Roles and responsibilities

Compliance

Vulnerability Analysis

Inventory

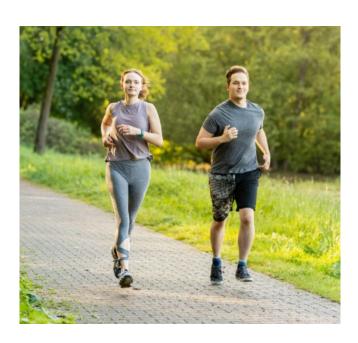
Software update

Technological validity

Contingencies exercised

Alternate Sites

Seizing "Peacetime"





Big Problems, Can Turn Into Big Oportunities

