Ransomware in Manufacturing

Dragos & SideChannel Series Pt. 2

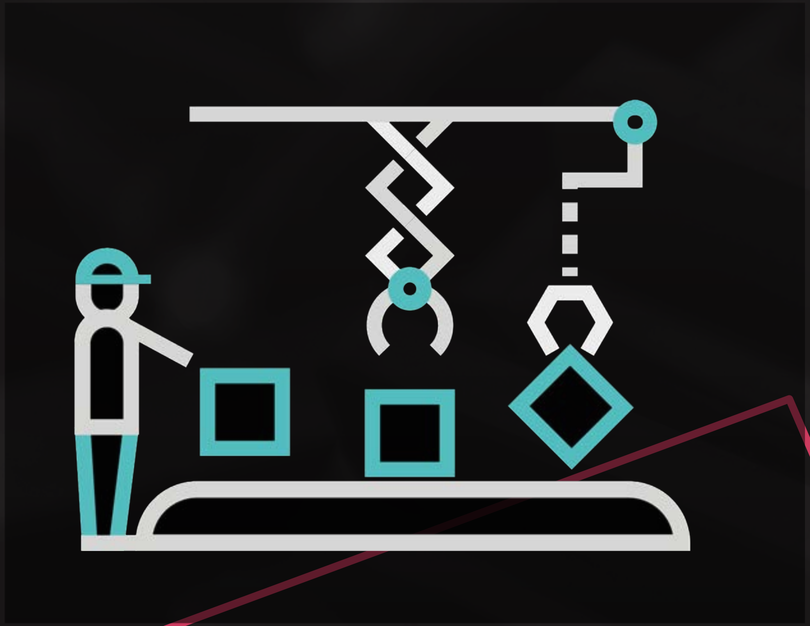
Brian Haugli, Co-Founder, SideChannel

Jason Christopher, Principal Cyber Risk Advisor, Dragos

Berardino Baratta, VP, Projects and Engineering, MxD

Evolution of Operational Technology (OT)

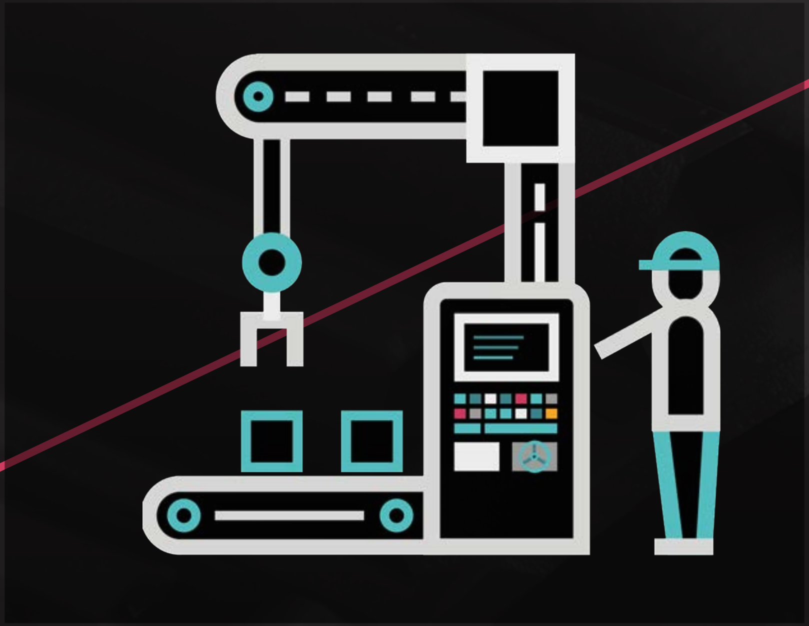
STAND-ALONE



standardization

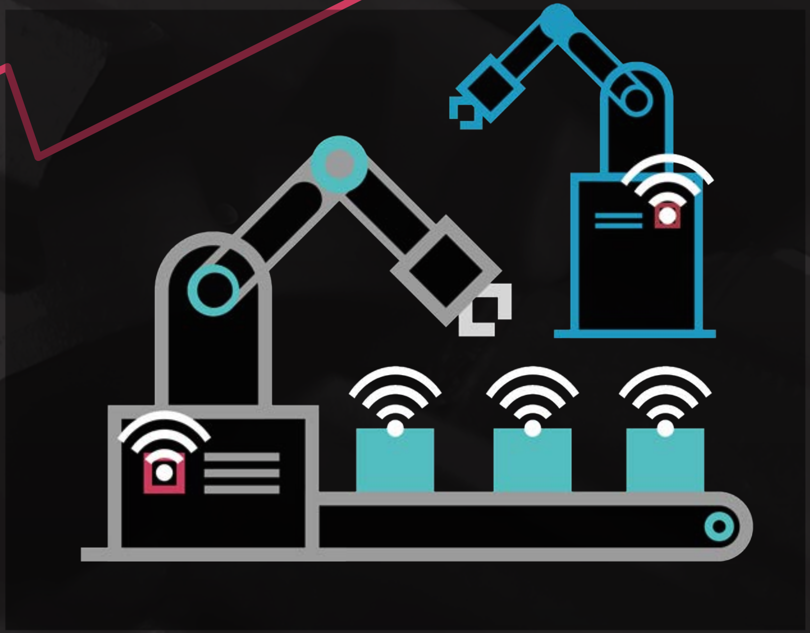
3rd Industrial Revolution
Automation of Production by Electronics

LOOSELY CONNECTED



DCS | Distributed Control System
SCADA | Supervisory Control & Data Acquisition

HIGHLY CONNECTED

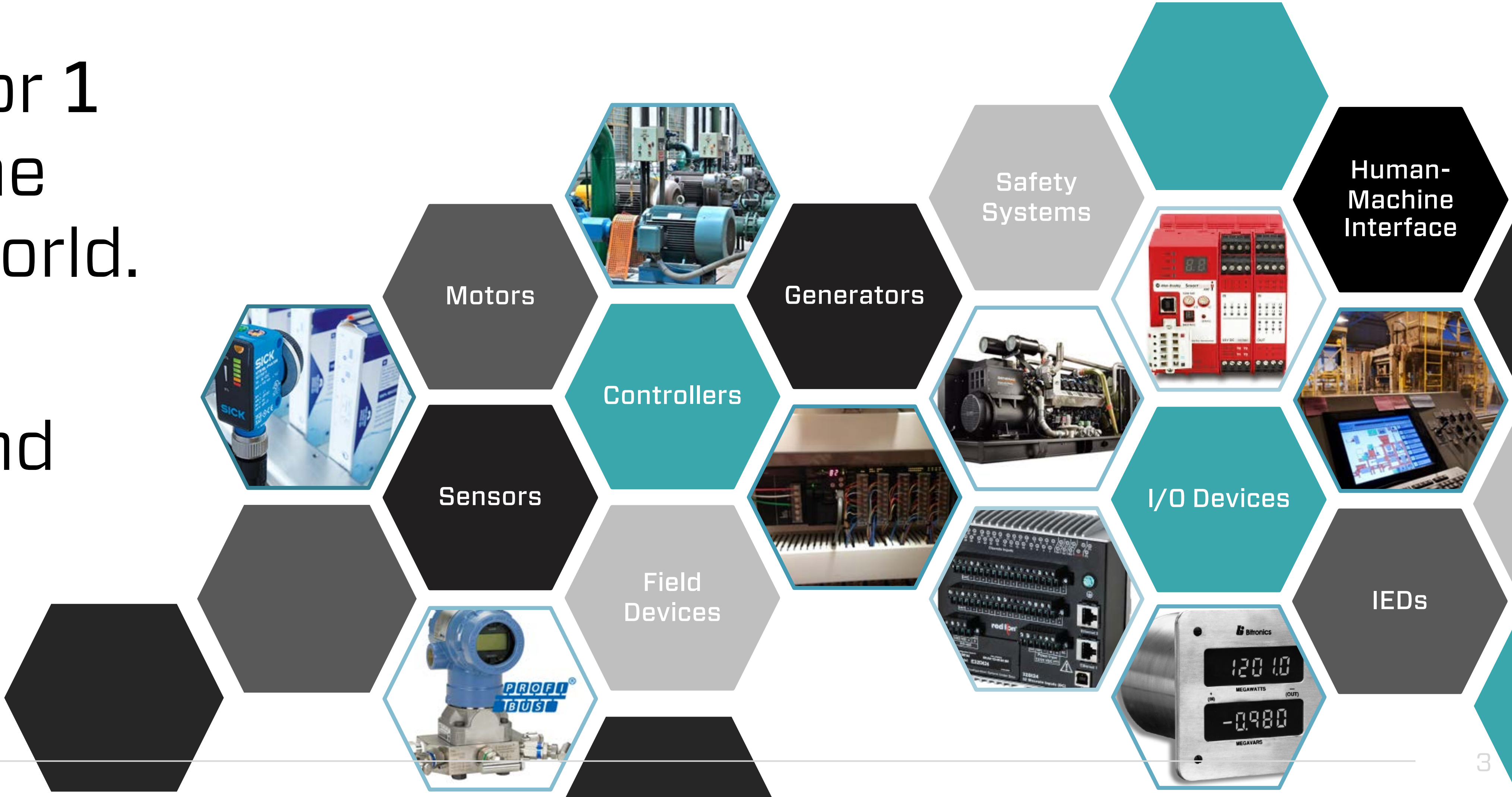


4th Industrial Revolution
Smart Connected Systems
“Industry 4.0” // “Industrial IoT”

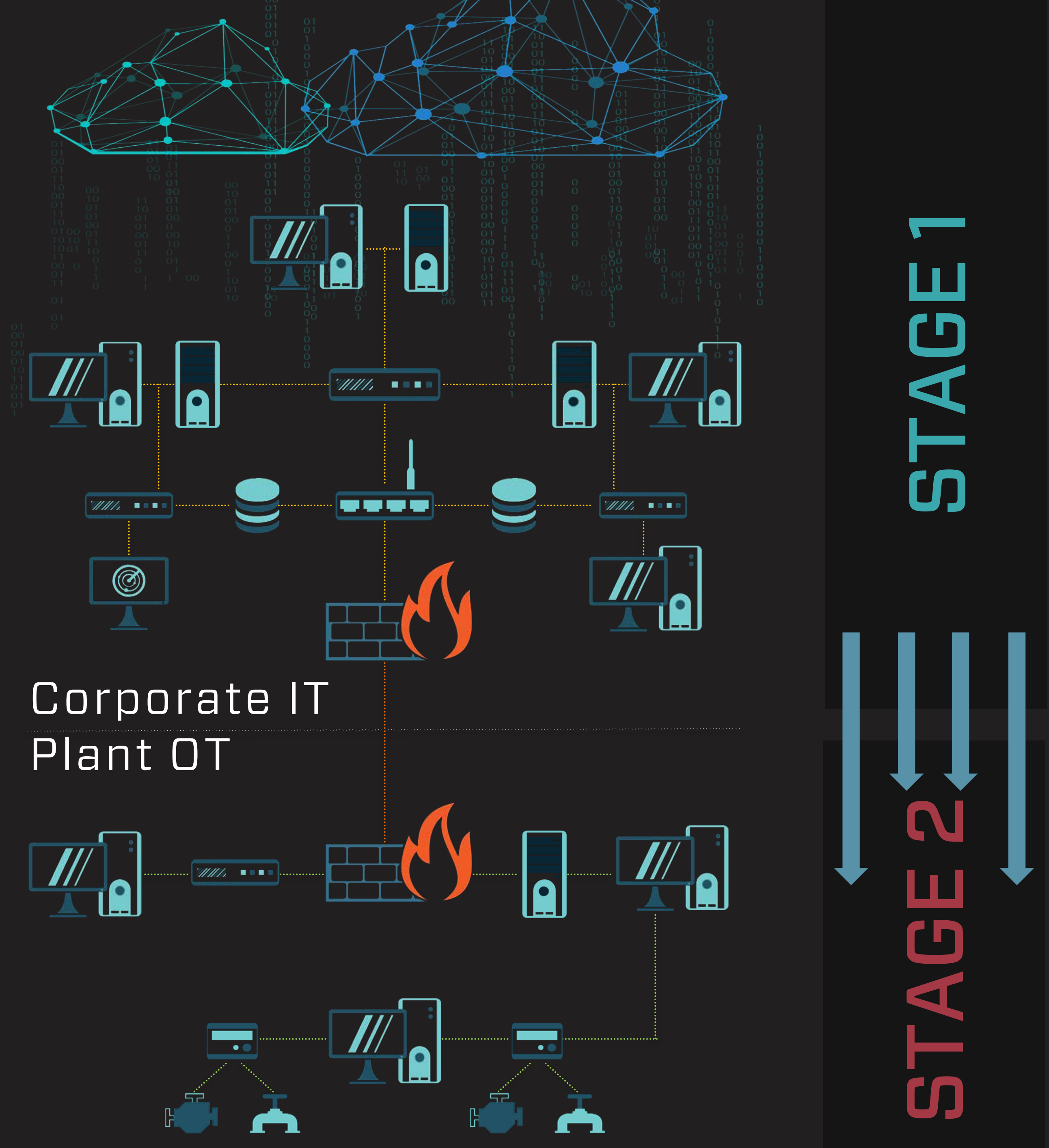
What are industrial control systems?

When a 0 or 1 impacts the physical world.

Devices and systems include:



- Safety Systems
- Human-Machine Interface
- Motors
- Generators
- Controllers
- Sensors
- I/O Devices
- Field Devices
- IEDs



Corporate IT

Plant OT

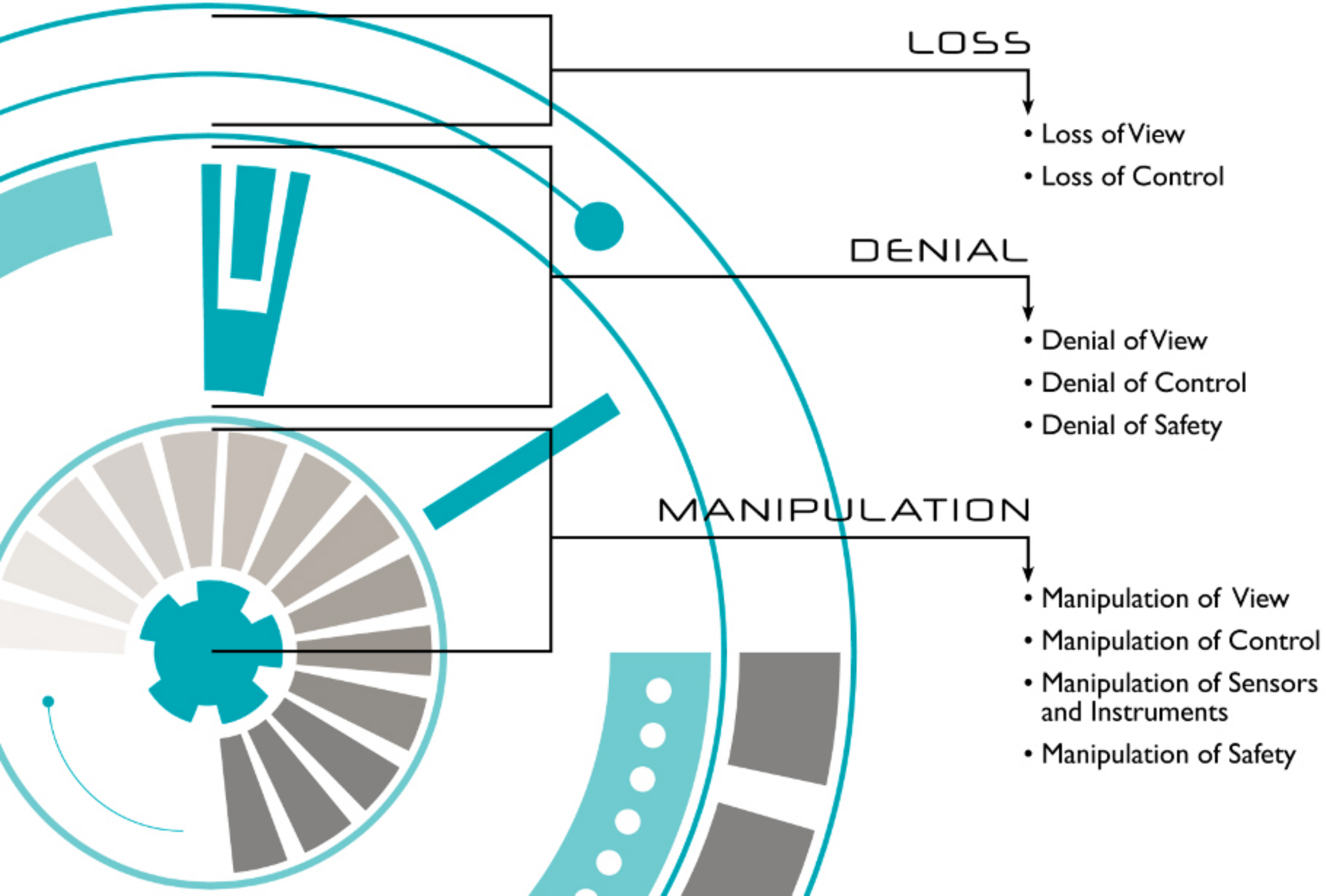
STAGE 1

STAGE 2

INDUSTRIAL ATTACKS: IT and OT

Stage 1 and Stage 2 work together to impact industrial processes, stretching across both IT and OT networks

Industrial Process Impacts



LOSS

- Loss of View
- Loss of Control

DENIAL

- Denial of View
- Denial of Control
- Denial of Safety

MANIPULATION

- Manipulation of View
- Manipulation of Control
- Manipulation of Sensors and Instruments
- Manipulation of Safety

For ICS-specific capabilities, the impact would be focused on *operational* impacts.

ENTER RANSOMWARE

Evolution of Ransomware

Pre-2017

- Primary targeting via phishing, malicious websites
- Single victim, single machine focus

2017-2018

- RISE OF THE WORMS
- Single victim machine, opportunistic targeting

2018-Present

- Interactive operations to attack corporate networks
- Hold entire networks hostage

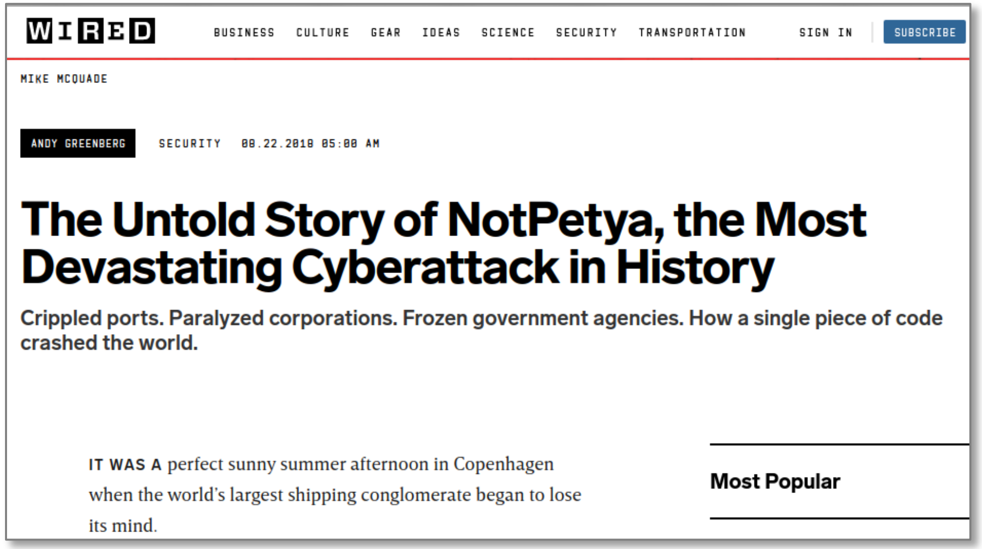
Source: J Slowik, TROOPERS20

WannaCry

150+ countries

230+ companies

Animated map from New York Times, accessed 2020-03-30: https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html



ANDY GREENBERG SECURITY 08.22.2018 05:00 AM

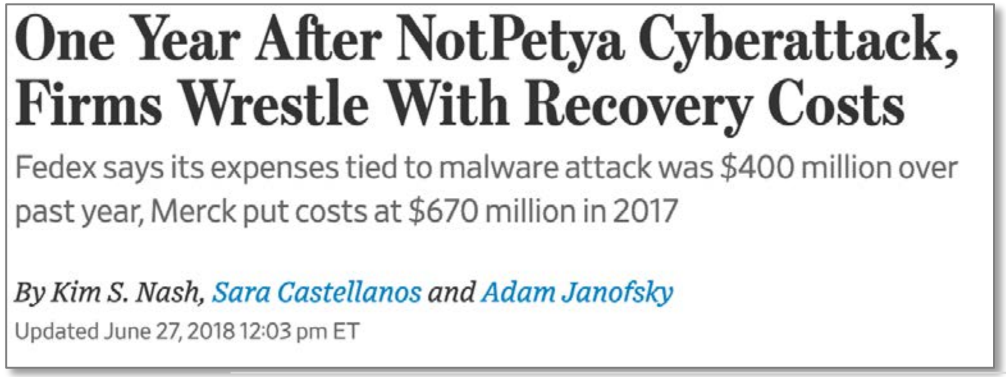
The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

Most Popular

FedEx® MAERSK MERCK Mondelēz International SAINT-GOBAIN Reckitt Benckiser



One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs

Fedex says its expenses tied to malware attack was $400 million over past year, Merck put costs at $670 million in 2017

By Kim S. Nash, Sara Castellanos and Adam Janofsky

Updated June 27, 2018 12:03 pm ET

NotPetya...
Not Ransomware

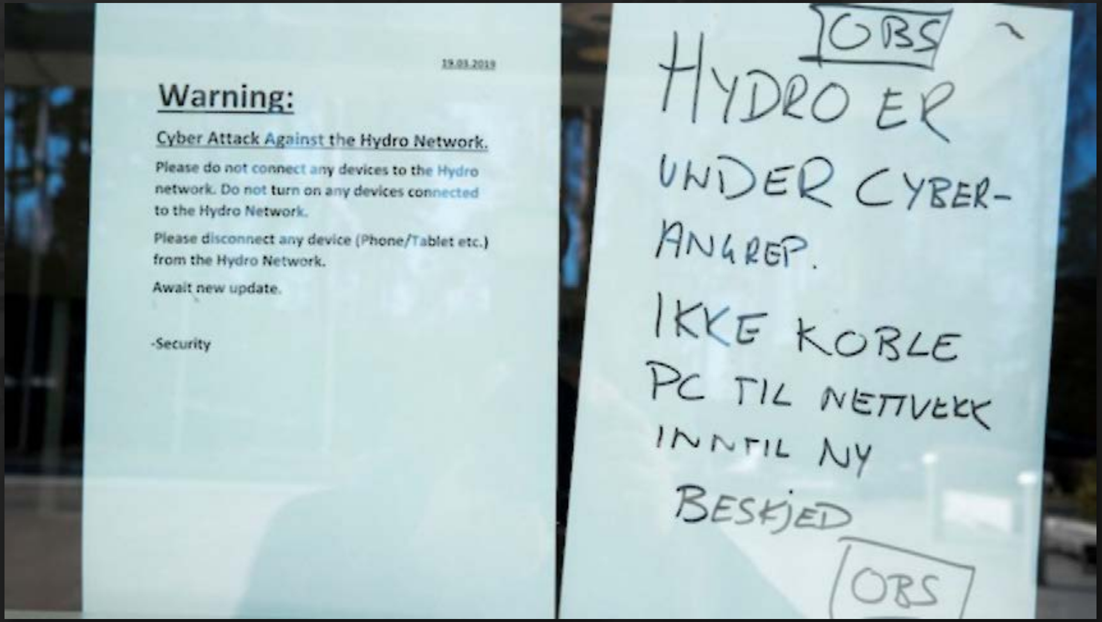
"Wiper disguised as ransomware," with increased collateral damage beyond any initial targets.

+$10B in estimated damages

2M computers impacted in 2HRs

+65 countries involved in response

Norsk Hydro & LockerGoga



19.03.2019

Warning:

Cyber Attack Against the Hydro Network.

Please do not connect any devices to the Hydro network. Do not turn on any devices connected to the Hydro Network.

Please disconnect any device (Phone/Tablet etc.) from the Hydro Network.

Await new update.

-Security

OBS

HYDRO ER UNDER CYBER-ANGREP.

IKKE KOBLE PC TIL NETTVERK INNTIL NY BESKJED

OBS

…at execution…

- Removes self, launches child process
- Writes ransom note

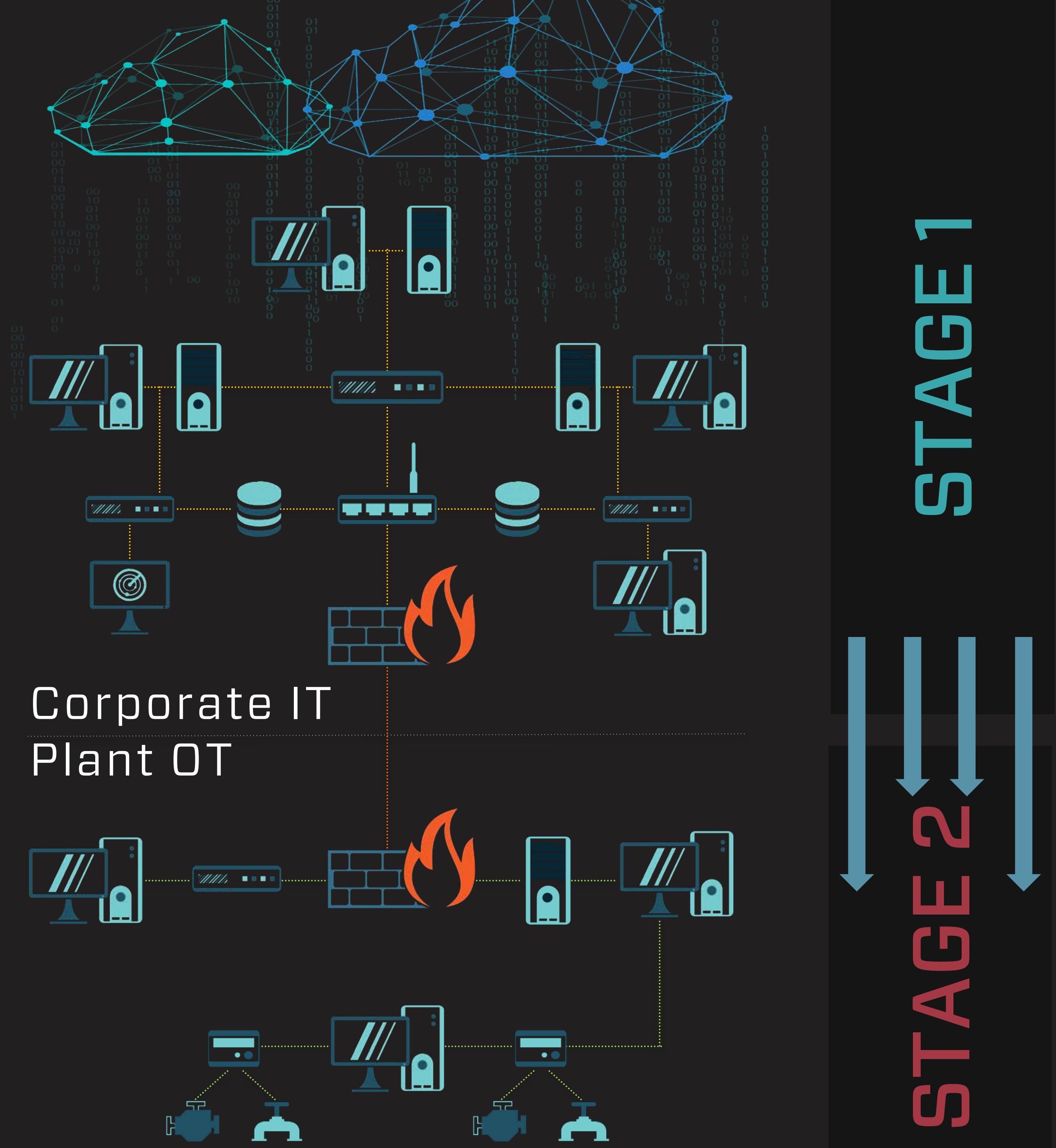
…through encryption…

- Encrypts files, binaries, etc
- Changes local user and admin credentials

…to lock out…

- Disables system network card
- Logs off all logged-in users

Read more here: https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/



IT-Centric RANSOMWARE in OT Systems

Again, think back to the ICS Cyber Kill Chain – there are no OT-specific knowledge or tools leveraged during these events.

OT was collateral damaged

Trends & Considerations

EKANS and ICS

- Ransomware with ICS-specific system processes highlighted

Ransom = $$$

- What are organizations willing to pay to unlock data?
- Whole networks?
- Entire industrial facilities?

Ransomware vs. Wiper

- Careful distinction, but would that change your behavior?
- Regardless of paying the ransom, would you ever trust that device again?

What's next?

- Ransomware evolution over the past few years shows trending towards bigger impacts

Thank You!

mxdusa.org

@MxDInnovates