RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: SBX4-W1

INSECURE CITIES AND ROGUE ROBOTS: THE IMPACT OF INDUSTRIAL IOT EXPLOITS

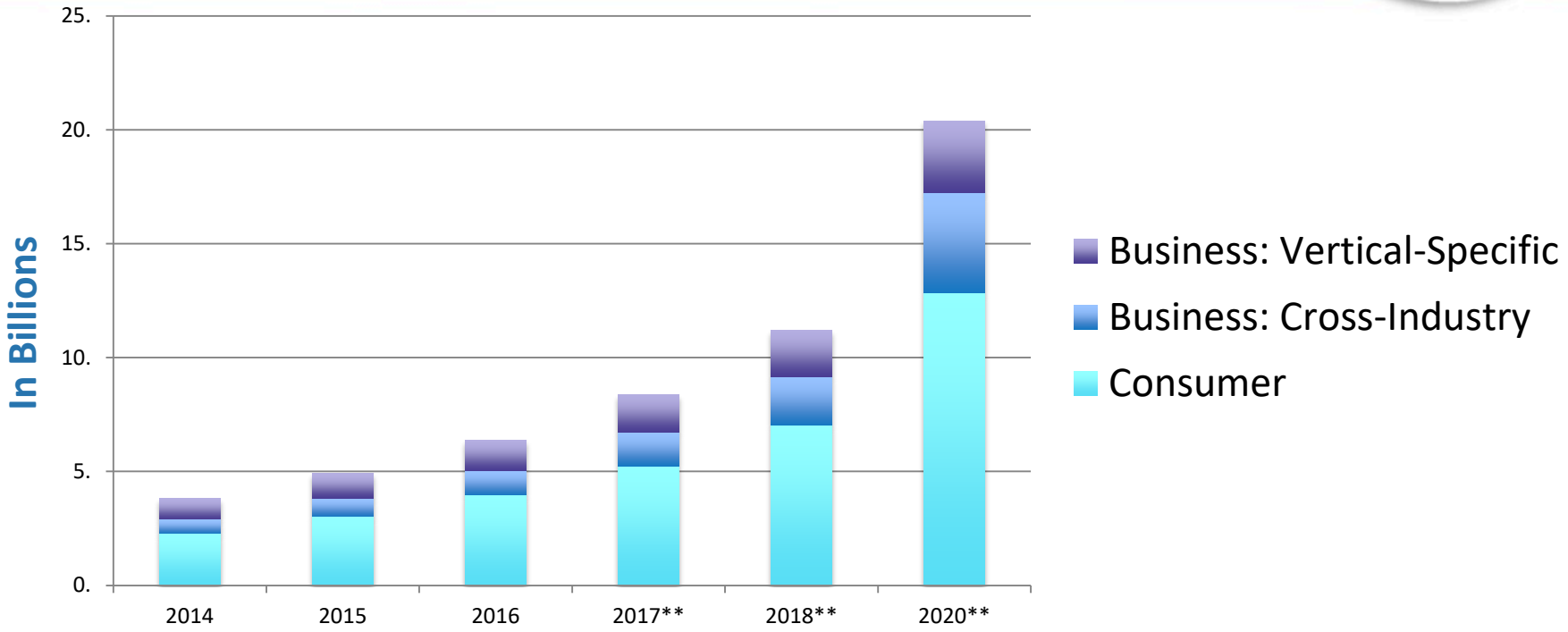
Ed Cabrera

Chief Cybersecurity Officer
Trend Micro
@Ed_E_Cabrera

By 2020, number of connected ‘things’ will be **26 billion**[1]

1. http://www.gartner.com/newsroom/id/2636073

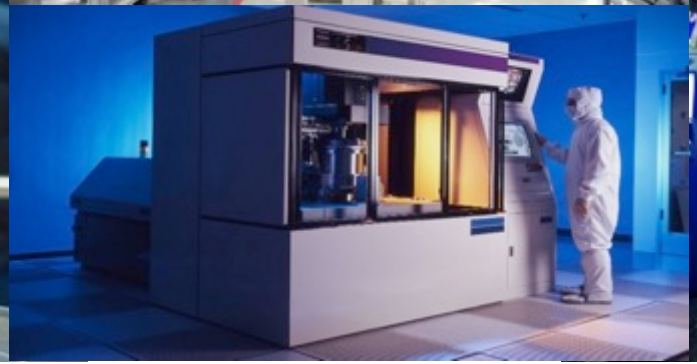
Connected IoT Devices by category 2014-2020



Source: Gartner

Smart Cities and Factories (Industry 4.0)




Industry 1.0 – 4.0

Mechanical Manufacturing

Stream machine replace human labor

Mass production

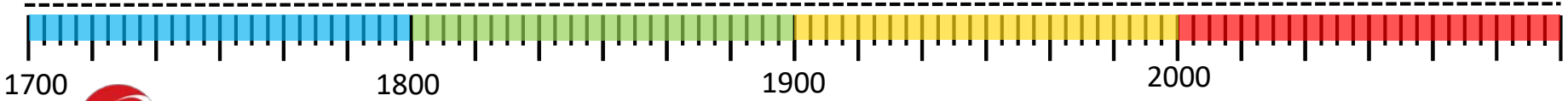
Electricity and the development of large capital goods industries

IT Automation

IT system deployment in production line

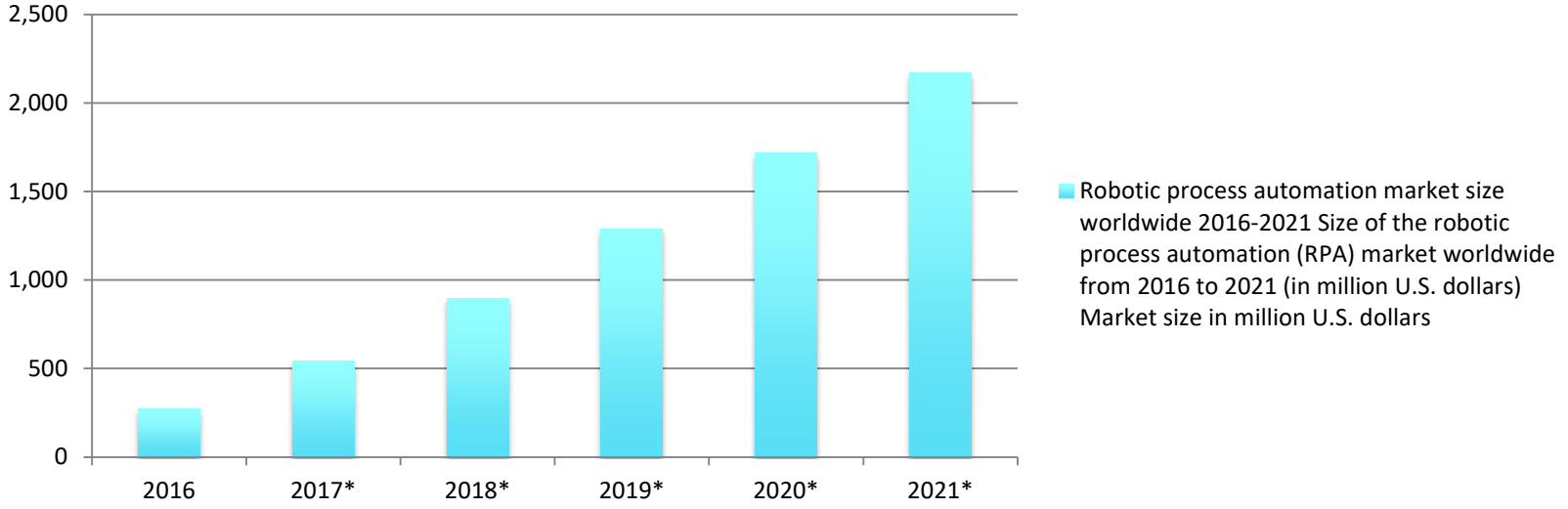
Cyber-Physical Systems

Smart factories with decentralized decision-making through IoT technologies



Robotic Automation

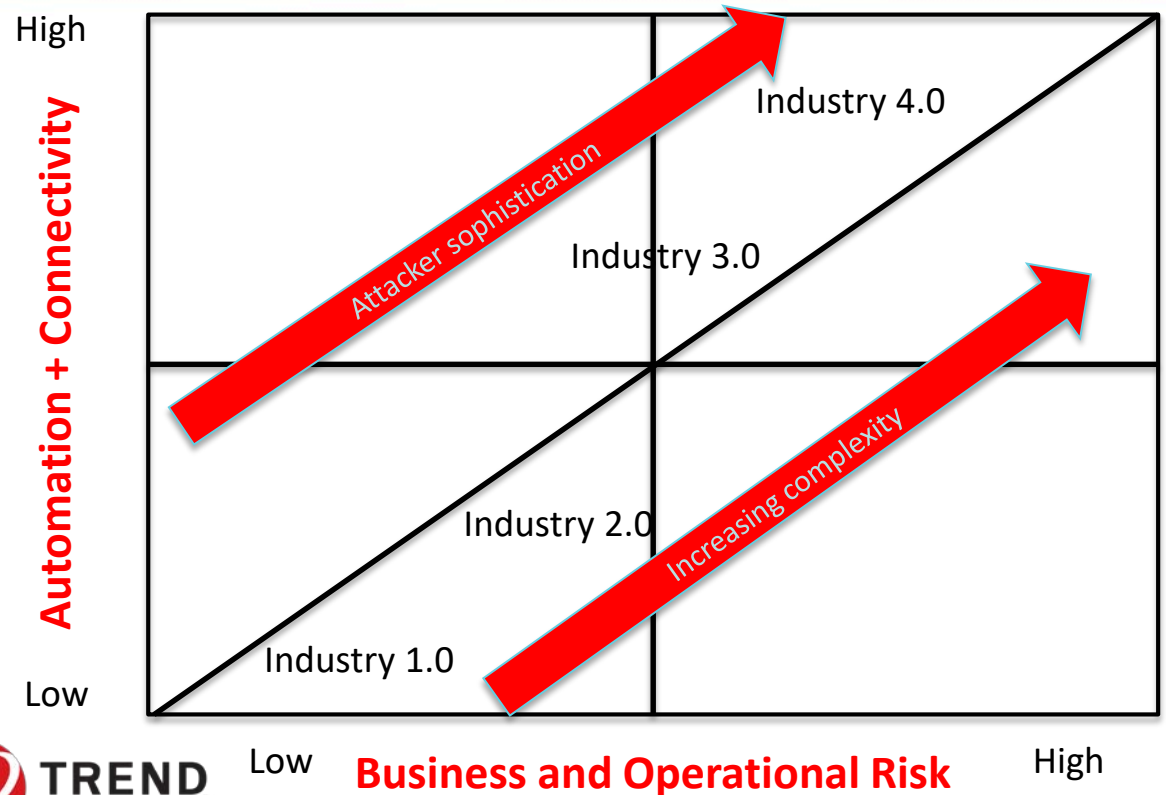
Robotic process automation market size worldwide 2016-2021



Source: HfS Research

SO WHAT'S THE RISK?

Evolution of Industry Risk



- Increased Automation
- Increased Connectivity
- Increased Complexity

+

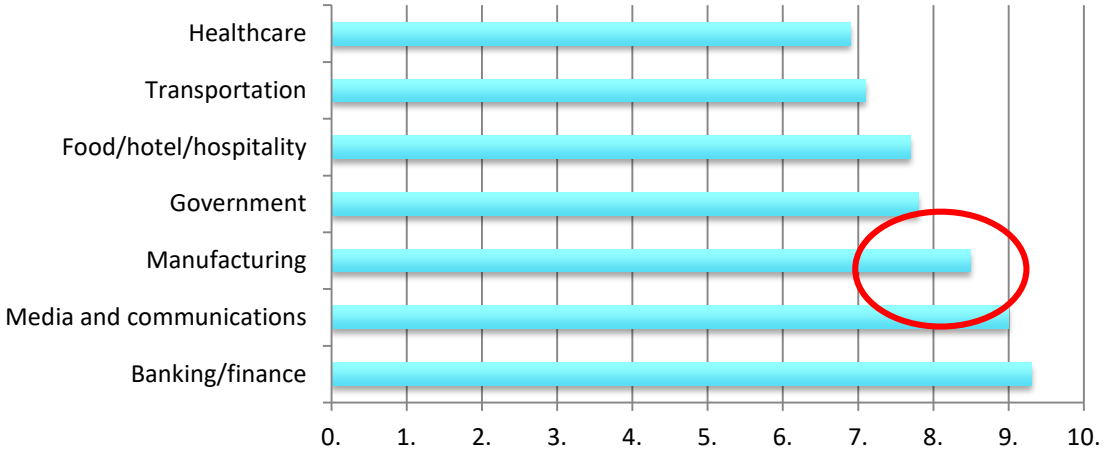
- Increased attacker sophistication

=

Increased RISK

Operational Risk

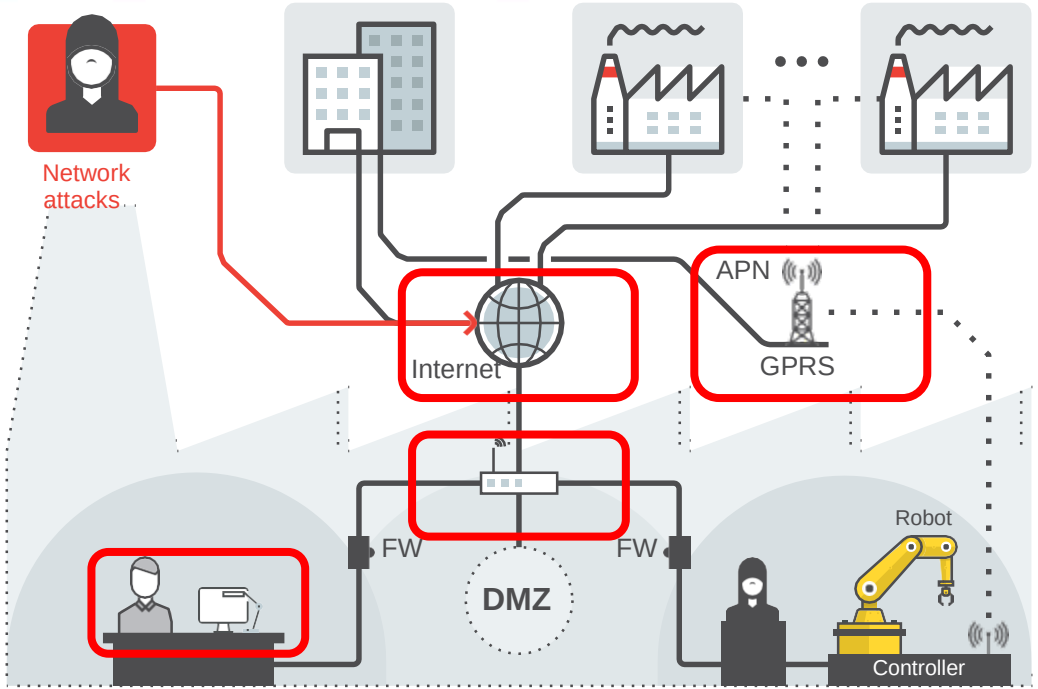
Global hourly server downtime cost 2017, by vertical industry



$8.5 Million Per Hour

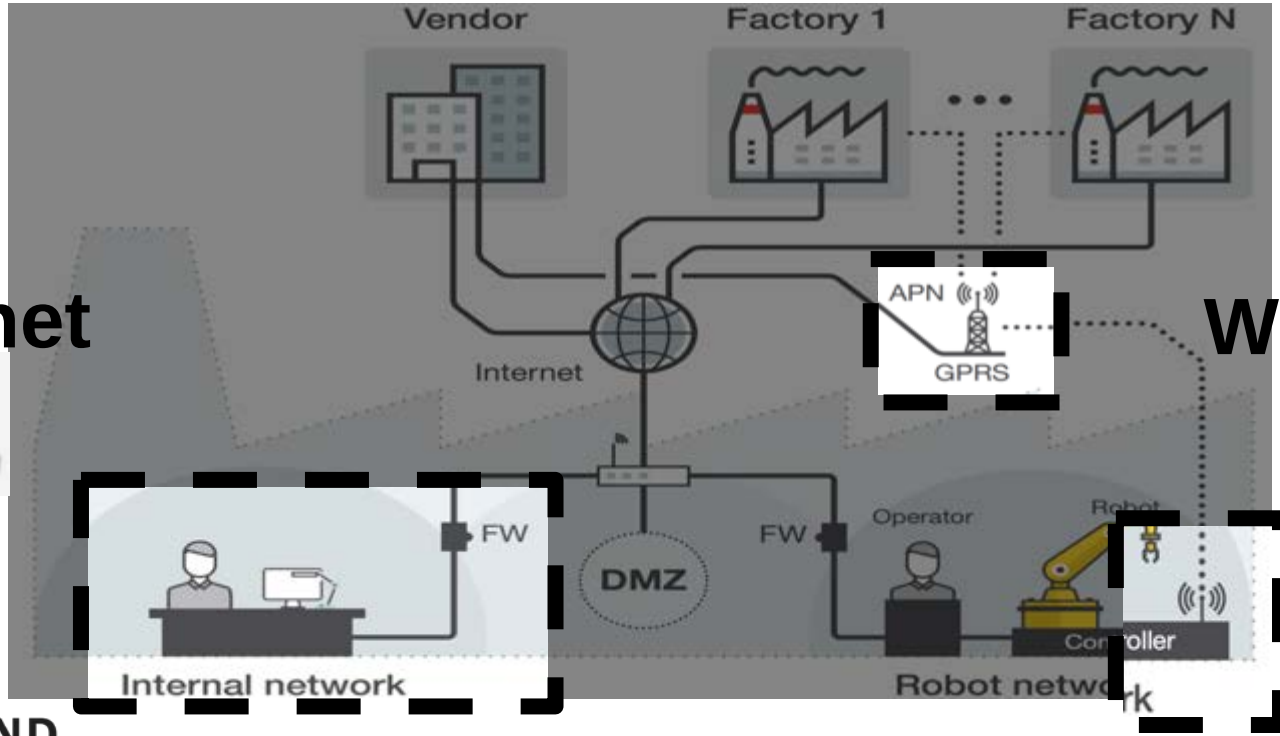
Source: Information Technology Intelligence Consulting

Threats to Smart Factories



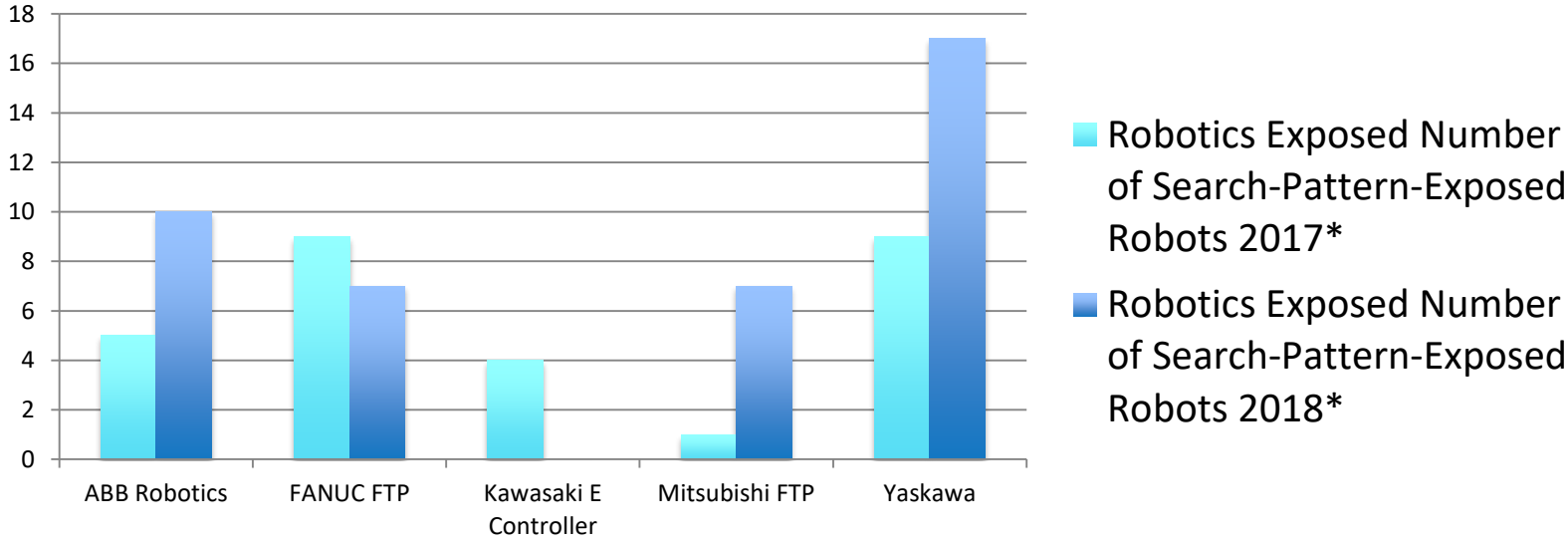
Threats to Smart Factories (Network)

Ethernet



Wireless

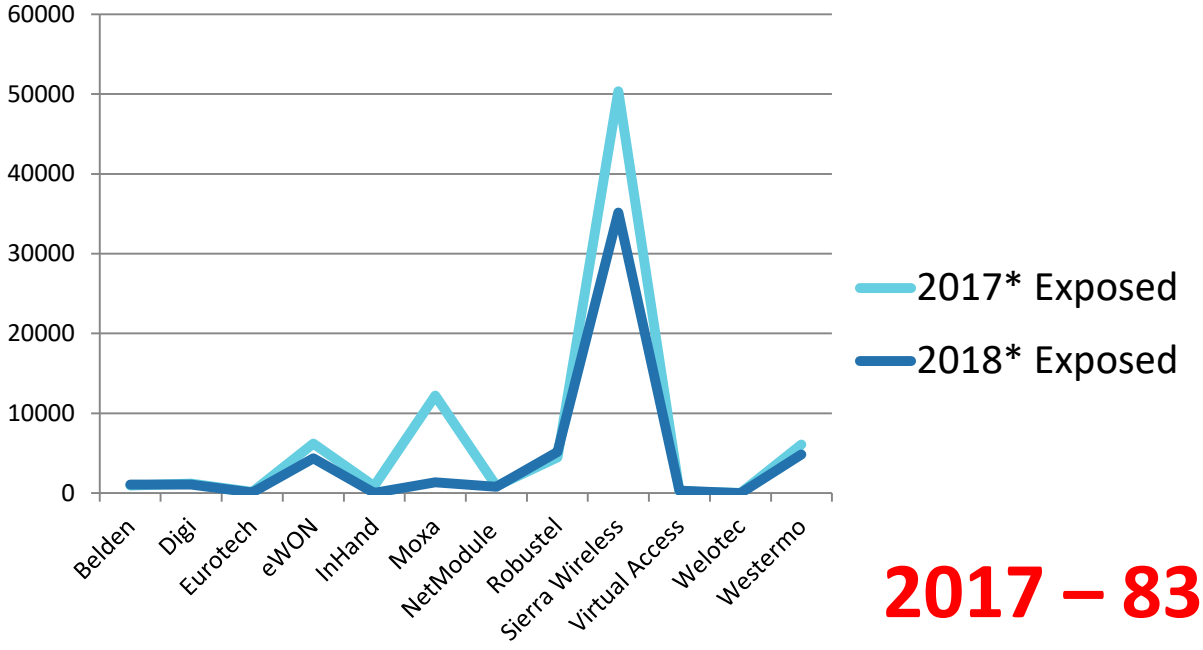
Robotics Exposed - Shodan



2017 - 28 Robots Exposed

2018 – 41 Robots Exposed

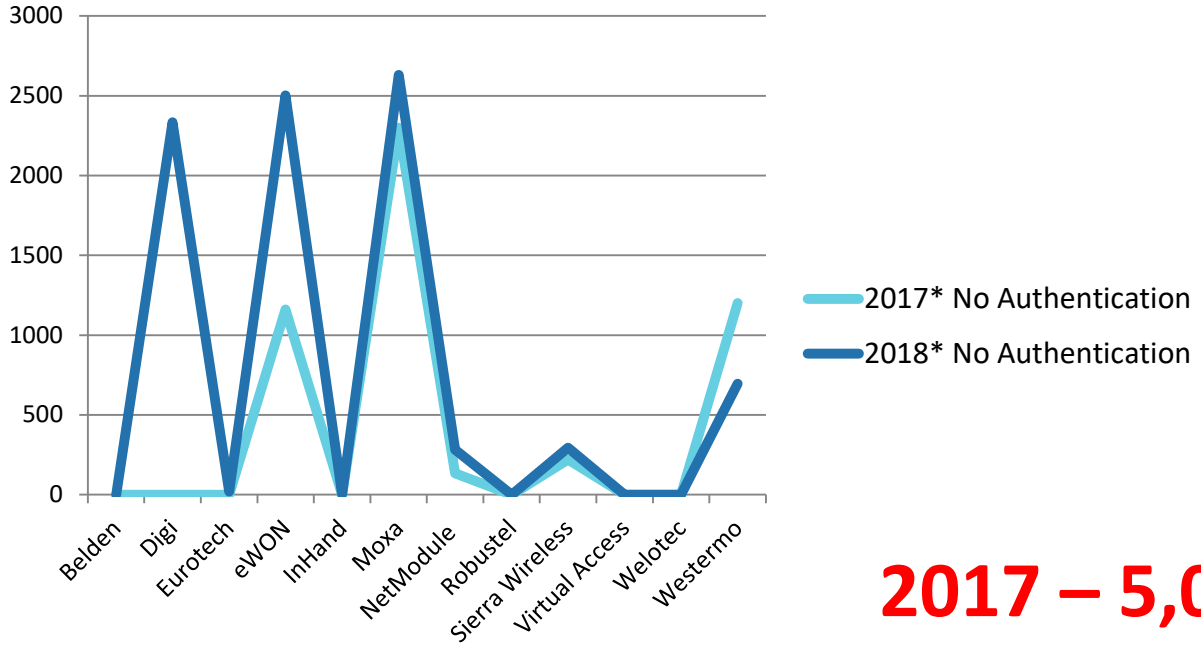
Remote Robots Exposed through Industrial Routers



2017 – 83,673 Exposed

2018 – 54,128 Exposed

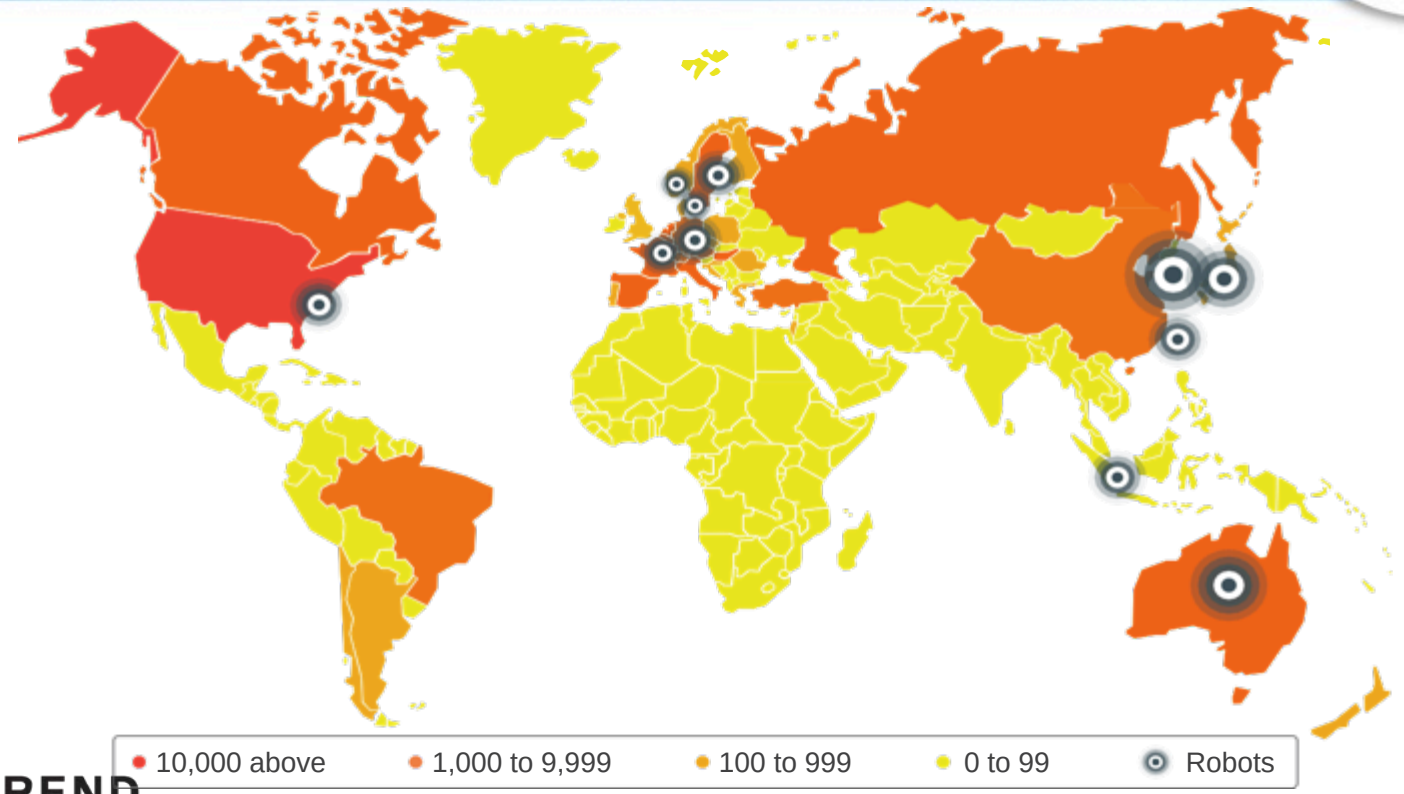
Industrial Routers with No Auth



2017 – 5,015 No Auth

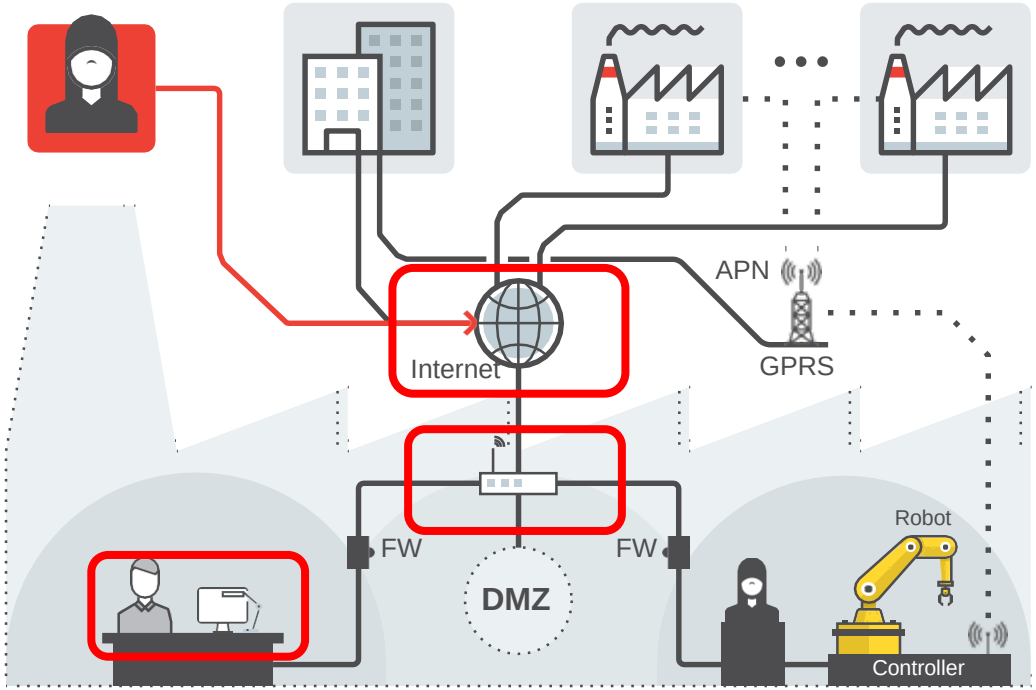
2018 – 8,758 No Auth

Exposed Robots and Routers

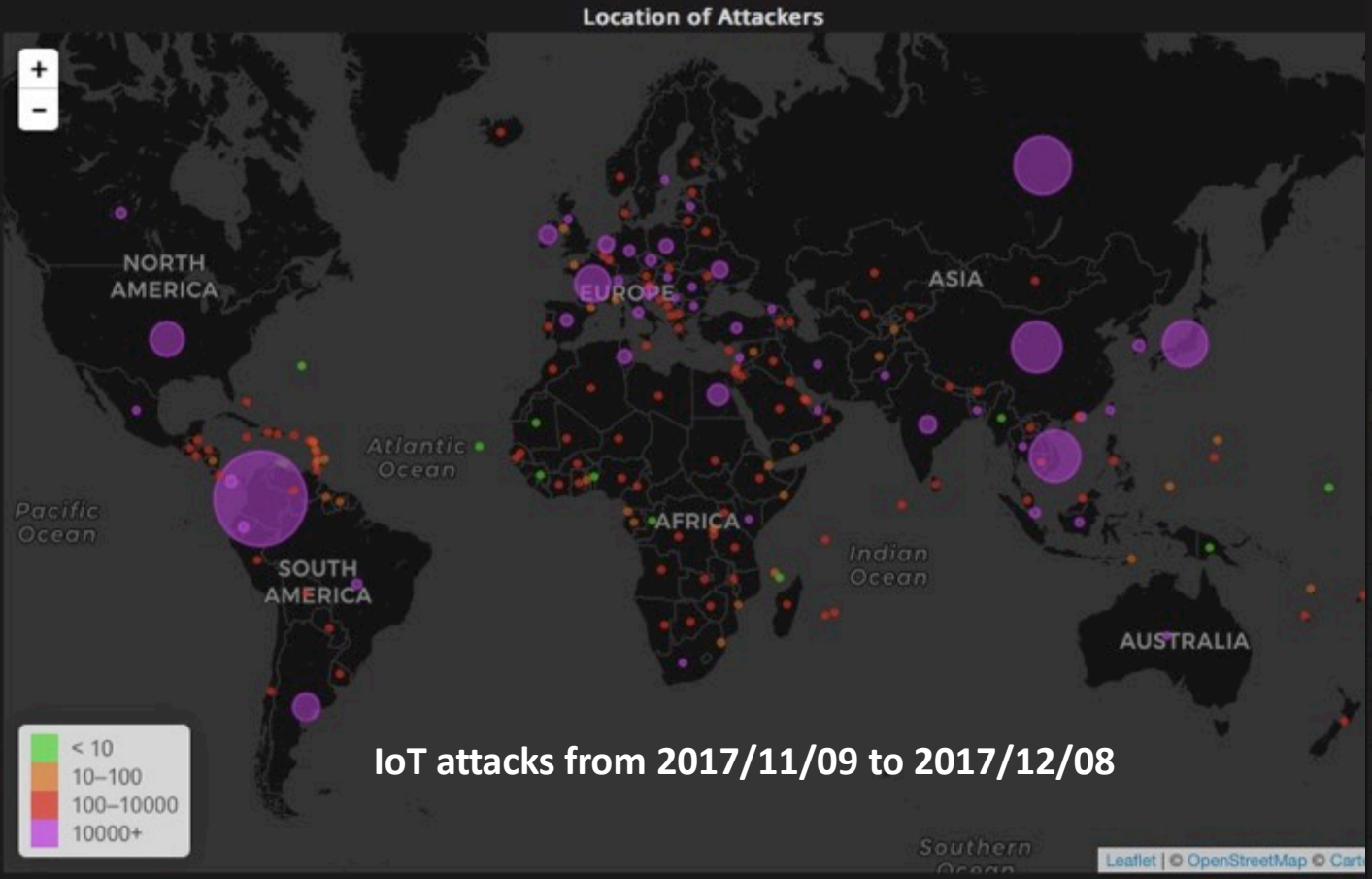


SO WHAT'S THE THREAT?

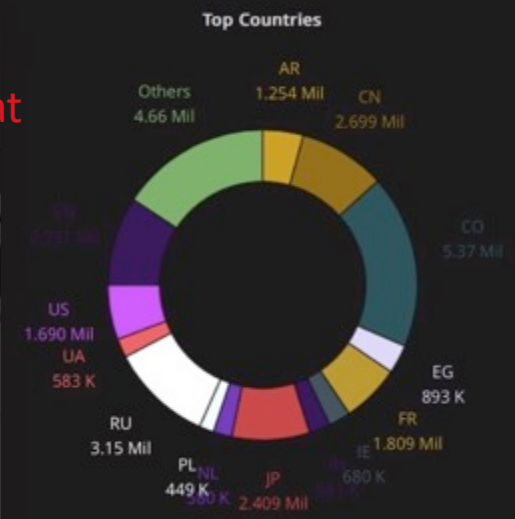
Threat Scenario 1:
Plant Disruption (IoT Botnets)



IoTRS Dashboard - Monitor the trend of global IoT threat



IoT attacks from 2017/11/09 to 2017/12/08



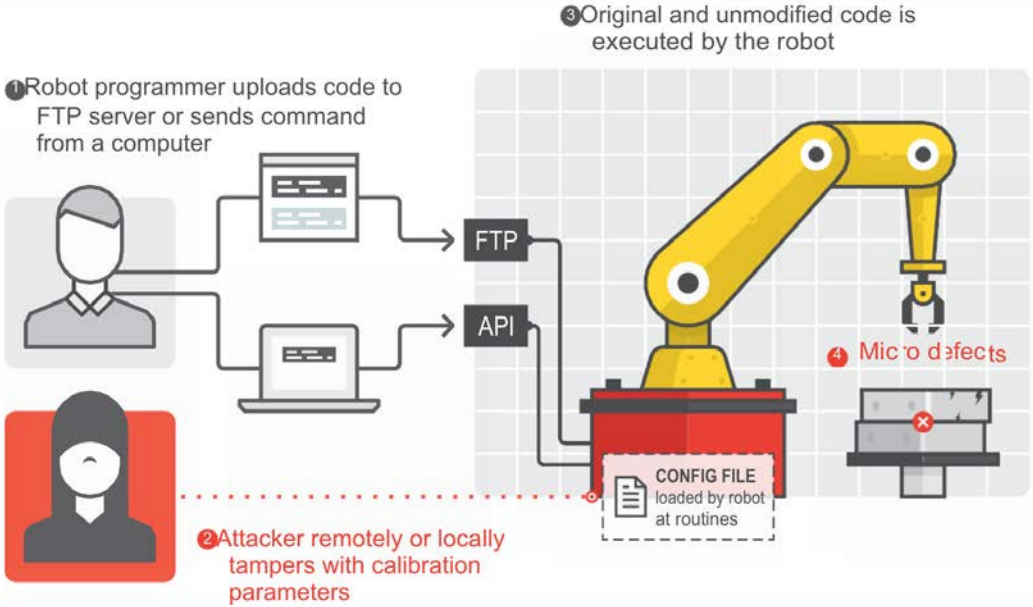
Top Attackers

IP	Country	Amount
185.188.207.12	RU	833.37 K
95.213.170.195	RU	321.78 K
185.13.37.96	FR	295.08 K
109.248.9.108	RU	271.98 K
193.201.224.206	UA	258.26 K
5.188.10.144	HR	258.25 K
195.22.127.83	PL	243.87 K
109.236.91.85	NL	239.95 K
195.154.151.12	FR	151.93 K
14.160.13.174	VN	151.80 K

Summery of Mirai attacks in South America and North African Countries (Nov 2017)

1. 1st wave was from Argentina
2. 2nd wave was from Columbia, Egypt, Tunisia, Ecuador, Panama, and Argentina,
3. The 2nd wave attack attempts shows similar patterns, especially in Columbia, Egypt, and Ecuador.
4. Attackers initiated attacks from South America and North African, and intended to compromise IP camera, NVR, and modems all over the world.

Threat Scenario 2:
Digital Extortion with ransomware or Altered Products



Threat Scenario 2:
Digital Extortion with ransomware or Altered Products

WannaCry ransomware causes Honda plant to shut down

It's still making the rounds.

Mallory Locklear, @mallorylocklear
06.21.17 in Security

6 Comments

2217 Shares

Sponsored Link

Miami, Flori
Tiny Compa
Year Old Ind

EverQuote Insurance Quotes

It's Like Eba
90 Se

Tophatter

Renault And Nissan Plants Hit By Massive Ransomware Attack

Stef Schrader
5/13/17 11:49am • Filed to: RENAULT

25.5K 101 12

Photo credit: Francois Mori/AP Images

TREND MICRO

RSAConference2018

Threat Scenario 3:
Physical Damage Sabotage

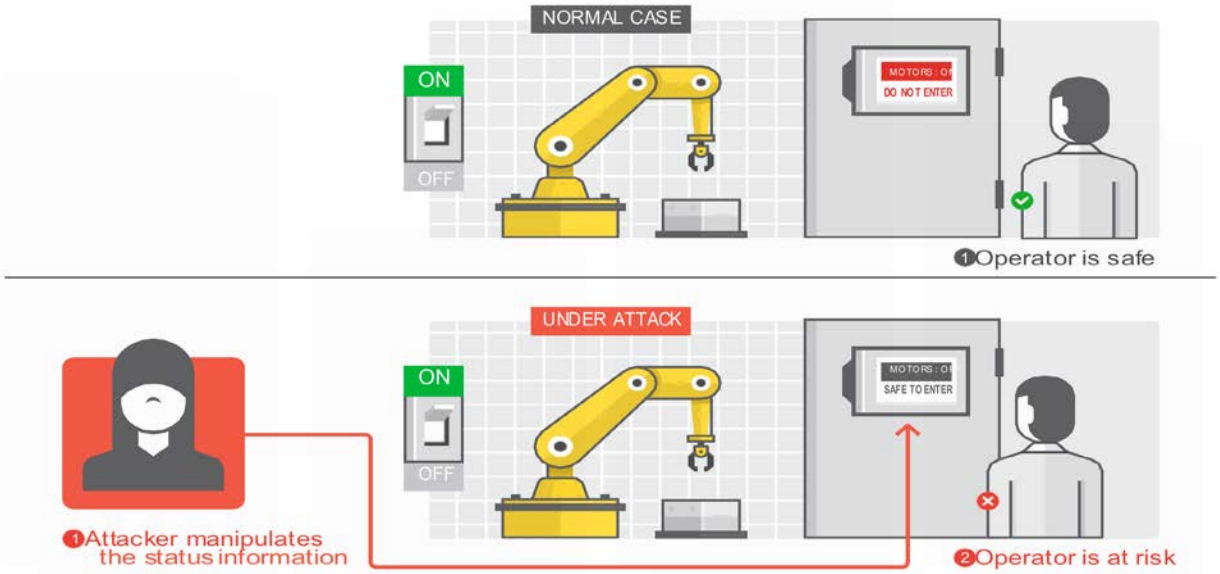


Figure 14. Attacker tampers with the user-perceived robot state to put the operator at risk

Threat Scenario 3:
Physical Damage Sabotage

Hackers Could Blow Up Factories Using Smartphone Apps

Researchers have found worrying security holes in ap companies use to control industrial processes.

Martin Giles

TRITON Wielding its Trident – New Malware tampering with Industrial Safety Systems

December 22, 2017

TRITON or TRISIS (detected by Trend Micro as TROJ_TRISIS.A)is a recently discovered malware that was designed to manipulate industrial safety systems and most notably was involved in shutting down an industrial plant's operations (reportedly in a country in the Middle East). According to reports, no harm was incurred so far by the victim in question as the plant's system safely shut down. However, the specific technology targeted is widely used in various industries, especially the energy sector, leaving other organizations vulnerable. Also, the system shutdown might have been inadvertently triggered as a result of exploration activity on the side of the attackers to learn how the system worked for future use.

Related

Threat Scenario 4:
Production Line Process Interference

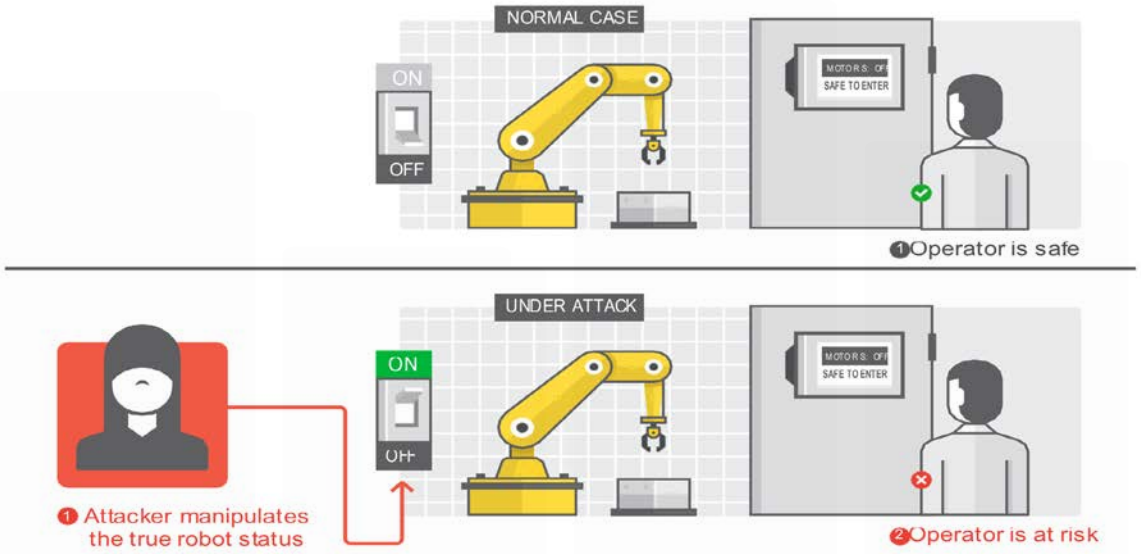
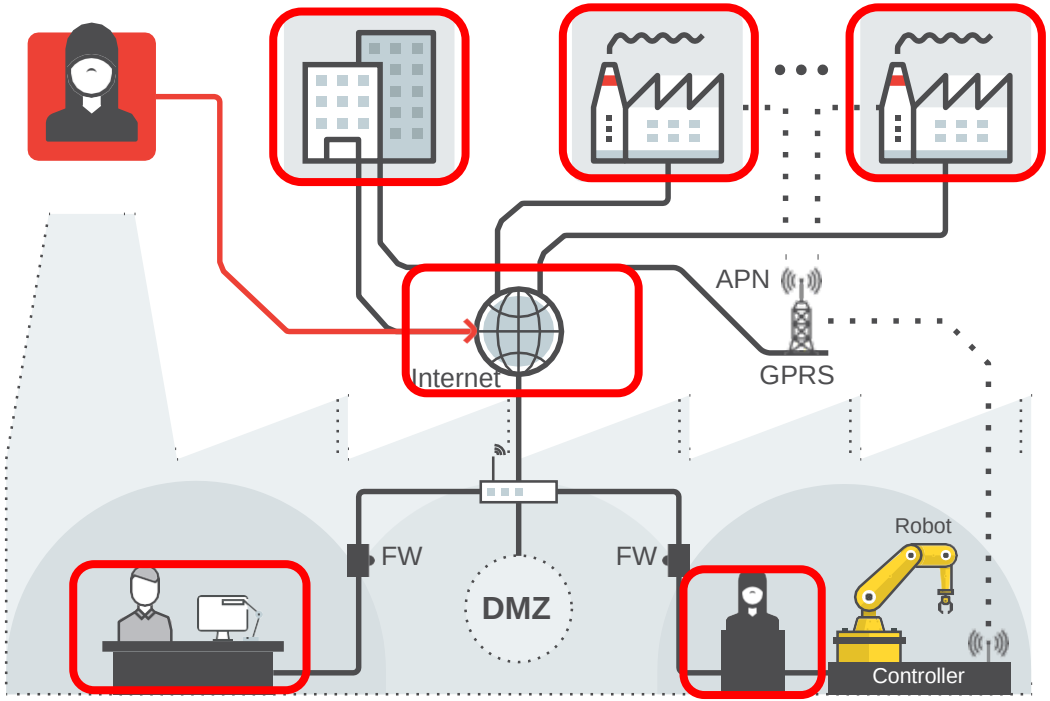


Figure 15. Attacker tampers with the actual robot state to put the operator at risk

Threat Scenario 5:
Sensitive Data Exfiltration



Threat Scenario 5:
Sensitive Data Exfiltration

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Alert (TA18-074A)
More Alerts

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Print | Tweet | Send | Share

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. It also contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by Russian government cyber actors on compromised victim networks. DHS and FBI produced this alert to educate network defenders to enhance their ability to identify and reduce exposure to malicious activity.

DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS).

ROGUE ROBOTS

Rogue Robots

Testing the Limits of an Industrial Robot's Security

Trend Micro FTR Research
Politecnico di Milano

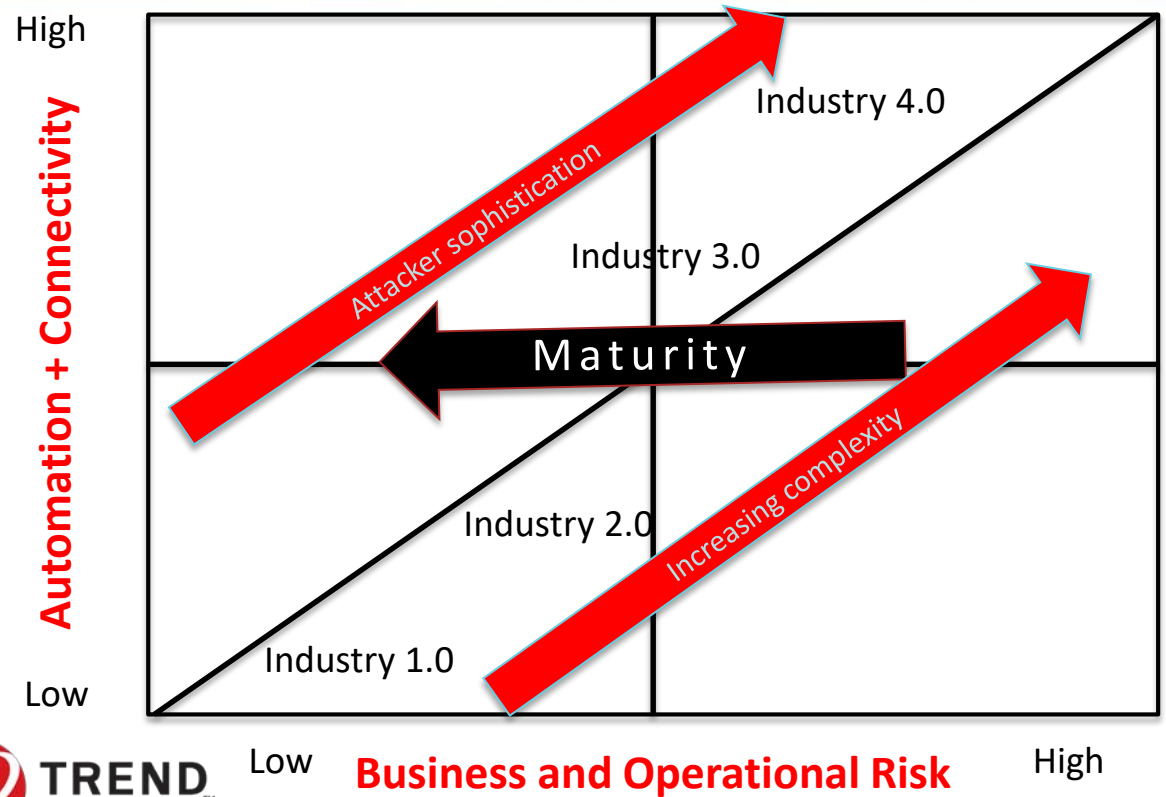
Federico Maggi
Davide Quarta, Marcello Pogliani, Mario Polino, Andrea M. Zanchettin, and Stefano Zanero

https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf

Attack Class and Description	Concrete Effects	Requirements Violated
Attack 1: Altering the Control-Loop Parameters **The attacker alters the control system so the robot moves unexpectedly or inaccurately.**	Defective or modified products	**Safety** **Integrity** **Accuracy**
Attack 2: Tampering with Calibration Parameters **The attacker changes the calibration to make the robot move unexpectedly or inaccurately.**	Robot damages	**Safety** **Integrity** **Accuracy**
Attack 3: Tampering with the Production Logic **The attacker manipulates the program executed by the robot to stealthily introduce a flaw into the workpiece.**	Defective or modified products	**Safety** **Integrity** **Accuracy**
Attack 4: Altering the User-Perceived Robot State **The attacker manipulates the status information so the operator is not aware of the true status of the robot.**	Operator injuries	**Safety**
Attack 5: Altering the Robot State **The attacker manipulates the true robot status so the operator loses control or can get injured.**	**Operator injuries**	**Safety**

SO HOW DO YOU REDUCE THE RISK?

Reducing Industry Risk



- Increased Visibility
- Increased Prevention
- Increased Detection
- Increased Response
- Increased Collaboration

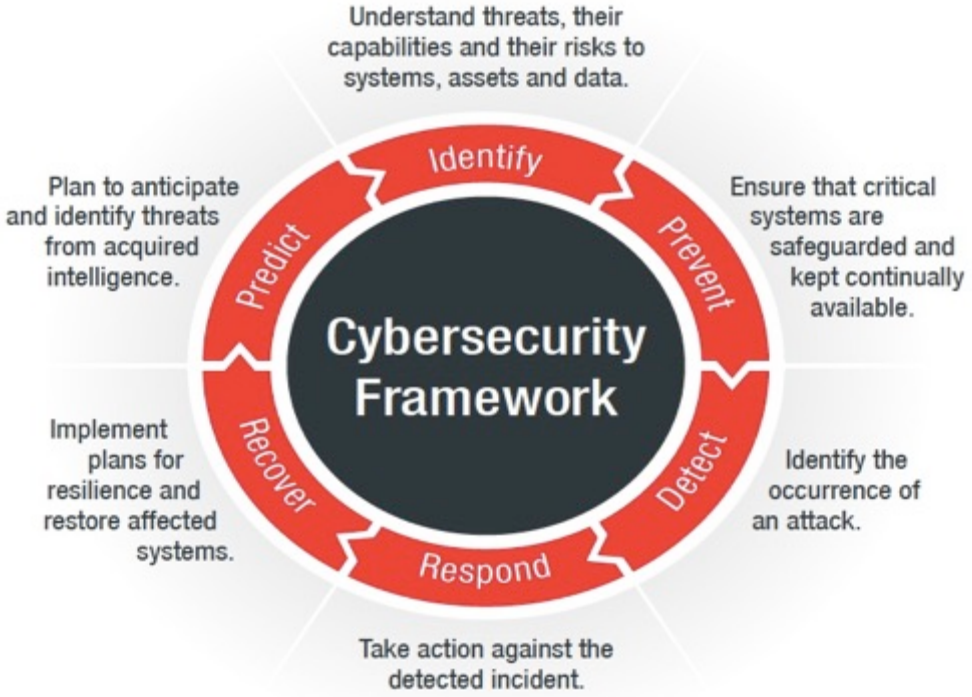
=

RISK Reduction

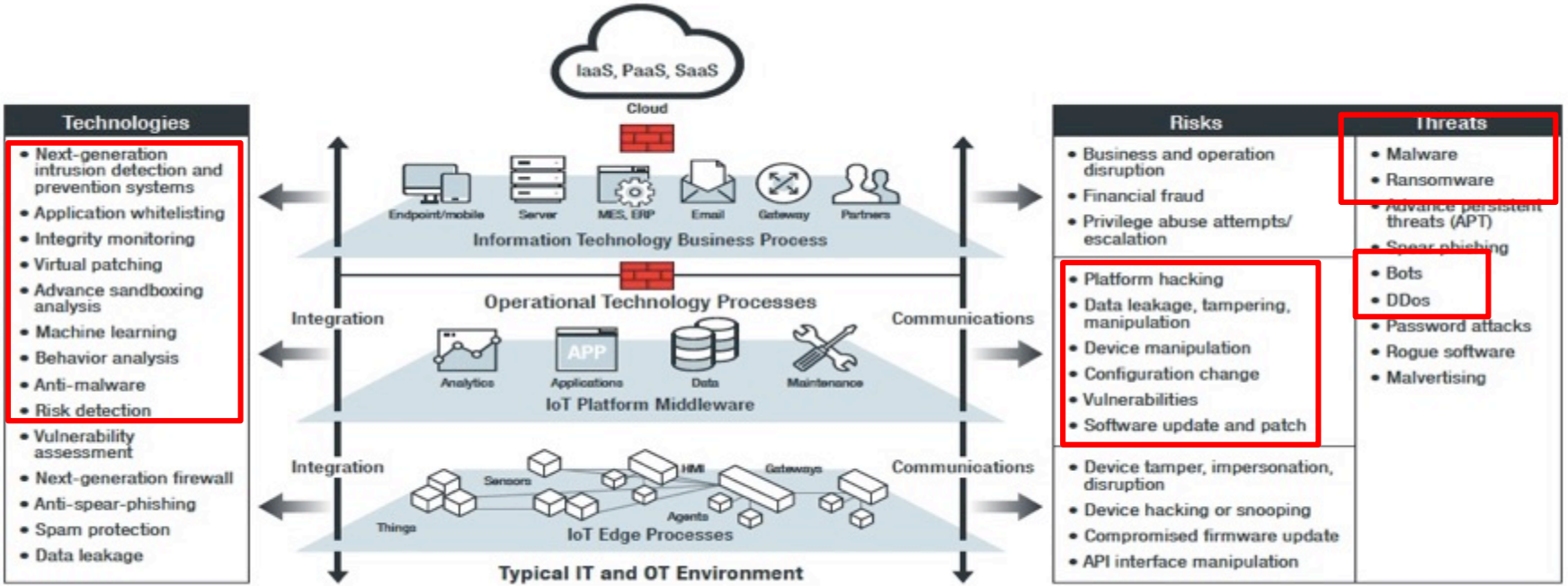
Reducing Industry Risk

- **Framework First**
  - Aligning IT/OT Risk Management with Business Goals, Strategies and Objectives
- **Design A Sound Foundation**
  - Understand CIA + AIC = Risk Resilience
  - Visibility through proactive joint risk assessments – red teaming exercises
  - Prevention through IT/OT Security Configuration and Architecture
  - Detection through joint SOC/NOC Fusion Centers
  - Response through joint IT/OT IR teams
  - Collaboration through cross functional security councils, crisis response teams, etc..
- **Partner Early and Often!**

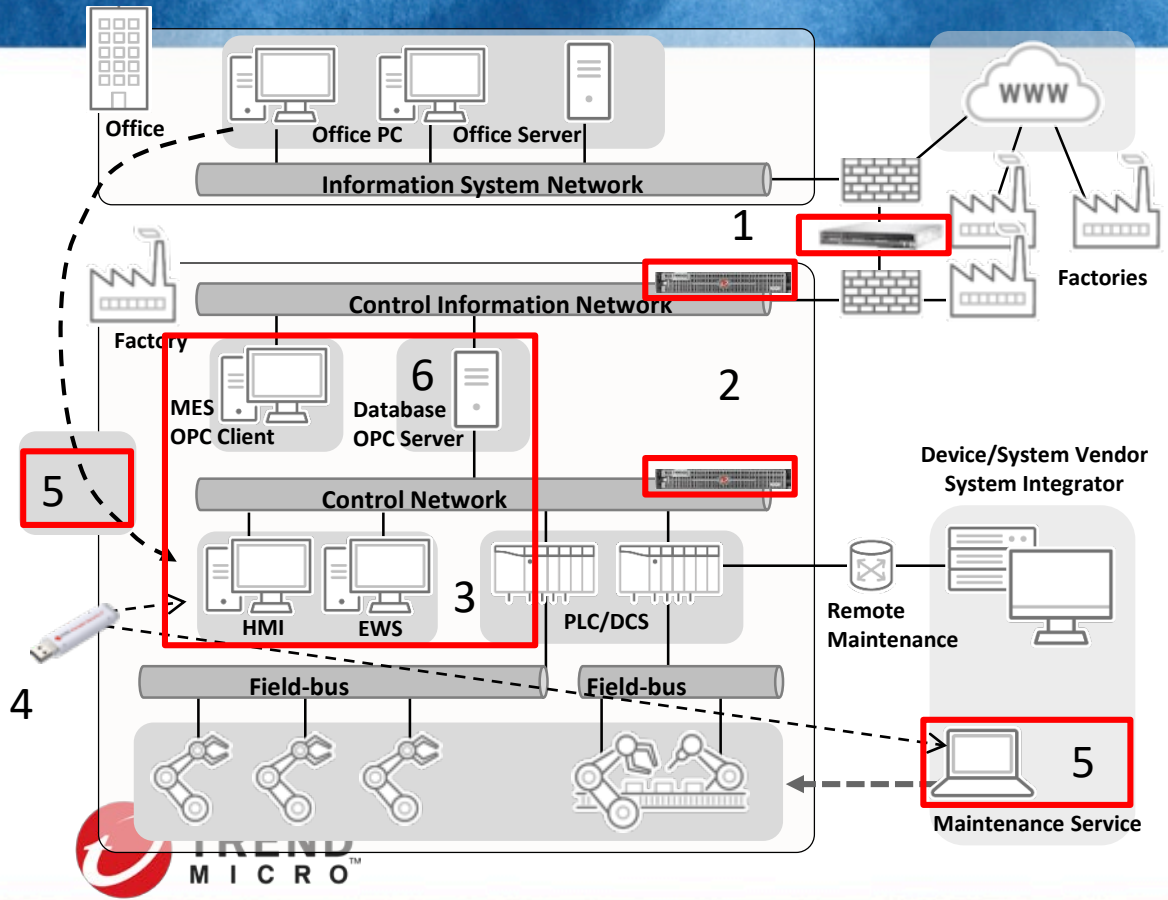
Framework First



Design a Sound Foundation



Deploy Risk Reducing Architecture



1. Next generation IPS against vulnerability attacks
2. Early anomaly and behavioral detection of threats
3. Lockdown anti-malware solution without using pattern file
4. USB stick anti-malware scanning solution without installation
5. Secure USB memory stick
6. Next generation server security solution

Deploy Risk Reducing Architecture

- **Zero Trust** – Utilizing IPS systems at the edge of OT systems
  - Connected Automation needs more than good security Configuration
- **Breach Detection** – monitoring and detecting malicious behavior on the enterprise side as well as on the Control Network Side
  - Speeding up detection and reducing dwell time
  - Correlating events and detections across both
- **Lockdown** anti-malware and whitelisting
- **USB anti-malware -** scanning without installation

Partner Early and Often!

THANK YOU