Recent Threats and Security Solution for a Smart Factory

Laksana Budiwiyono, Country Manager

Conference at Kementerian Perindustrian RI
Jakarta, 24 Oct 2018
Trend Micro

- 30 years focused on making “A World Safe for Exchanging Digital Information”
- Headquartered in Japan, Tokyo Exchange Nikkei Index
- Annual sales of approximately $1.3B US, consistently profitable
- Customers include 45 of top 50 global corporations
- 6000+ employees in over 50 countries

500k commercial customers & 250M+ endpoints protected
Agenda

• Recent Threats and Incidents
  – Incidents
  – Increasing risks by IIoT and Industry 4.0

• Trend of Security for a Factory
  – 3 Directions of security measures
  – Customer cases
Threats and Incidents
Recent Incidents and News

• RANSOMWARE disrupted factories

• COINMINER is seeking next target

• Malware infection in a factory is NOT minority
# RANSOMWARE disrupted Factories

<table>
<thead>
<tr>
<th>Date</th>
<th>Ransomware</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>May, ’17</td>
<td>WannaCry</td>
<td>Japanese and French major car manufacturer’s factories shutdown in Europe and German train related systems compromised.</td>
</tr>
<tr>
<td>Jun, ’17</td>
<td>Japanese major car manufacturer’s factory shutdown a whole day in Japan.</td>
<td></td>
</tr>
<tr>
<td>Jun, ’17</td>
<td>Petya variant</td>
<td>American pharmaceutical company’s factory shutdown, and it brought late shipment and drop of stock price.</td>
</tr>
<tr>
<td>Aug, ’18</td>
<td>WannaCry Variant</td>
<td>Taiwanese semiconductor manufacturer’s factories shutdown in Taiwan and caused about $200M loss.</td>
</tr>
</tbody>
</table>

![WannaCry](image1.png)

![Petya Variant](image2.png)
Ref: WannaCry cases

Production line

HMI in a factory

ATM

Payment terminal in a gas station

Railway control center

Train Information Display

Ref: http://b0n1.blogspot.jp/2017/05/wannacry-ransomware-picture-collection_17.html
COINMINER is seeking next target?

COINMINER malware hits monitoring systems at European water utility*¹. Detections of COINMINER is increasing now*²

Cryptocurrency-mining tool detections world wide

Q1 2017: 37,047
Q2: 37,500
Q3: 55,538
Q4: 270,788
Q1 2018: 333,538

Source:
*¹ https://www.securityweek.com/cryptocurrency-mining-malware-hits-monitoring-systems-european-water-utility
*² Cryptocurrency-mining tool detections world wide, Trend Micro, May, 2018
Malware infection in a factory is NOT minority

U = 143, who manage and operate industrial control systems in FA/PA.
## Ref: Another incidents in Industrial Control Systems

<table>
<thead>
<tr>
<th>Industrial Facility</th>
<th>Water Treating Plant</th>
<th>Railway Traffic Control System</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Impact</strong></td>
<td>Loss of control for 3 months (1ML of polluted water emission)</td>
<td>Shutdown of train service</td>
</tr>
<tr>
<td><strong>Cause</strong></td>
<td>Unauthorized access</td>
<td>Blaster malware</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>Wireless link</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Car Factory</th>
<th>Steel Plant</th>
<th>Chemical Plant</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Impact</strong></td>
<td>Steam turbine control system stopped</td>
<td>8 hours of monitoring incapability</td>
</tr>
<tr>
<td><strong>Cause</strong></td>
<td>DOWNAD/Conficker malware</td>
<td>PE_SALITY malware</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

### Impact Descriptions:

- **Centrifugal separator crash**: 13 production line stopped/ $14M loss
- **Stuxnet malware**
- **Zotob malware**
- **USB flash drive or office network**
- **Steam turbine control system stopped**
- **DOWNAD/Conficker malware**
- **Unknown**

**Source:**
- [http://www.securityincidents.org](http://www.securityincidents.org)

---

**Copyright 2018 Trend Micro Inc.**
Business Impacts of Incidents in a Factory

Not only financial damage but also company reputation and safety are affected. It is about corporate management issue.

- Delay of delivery of goods
  - Factory shutdown

- Recall
  - Defectives shipping

- Low physical safety
  - Malfunction

- Recovery costs
  - Infection
Why they couldn’t protect a factory?

• **No security or Not enough security**
  - Common concept: device vendor should have security responsibility
    • But actual damages come to asset owners and customers
  - Myth: closed environment is safe
    • Infection from USB memory stick or maintenance PC
    • Unmanaged network connection and devices
  - IS department: factory is out of scope
  - Long-term lifecycle
    • Legacy OS, non-patched systems
    • No program update due to the importance on Availability
  - Device vendor prohibits to install other software
  - Security product: signature file is never up-to-date

• **Not enough operational rules**
  - Rules are hard to thoroughly uphold and complex
Why did damage expand in a factory?

- Infection through Network and/or USB flash drive
- One-off device and difficult to replace it
- No Incident response rule and organization
- Fail to notice a malicious behavior
- Fake UI (i.e., STUXNET)
Increasing Risks by IIoT and Industry 4.0

Open OS and network connection with standard protocol are deployed

**Benefit**
- Visualization
- Predictive maintenance
- Inventory optimization
- Mass customization

**Disadvantage**
- Increase of shutdown risk
Trend of security for a factory
Background of security deployments

• Risk management by executives
  – Factory shutdown damages in company reputation
    • Shutdown 1 hour = Loss of USD few million
  – Risk of lawsuits
  – Government’s enforcement

• Mind-set change in OT admin
  – Cyber incident causes an identical result, a factory shutdown, as physical incident
3 Direction of Security Measures

1. Establish Security Standard

2. Defense in Depth

3. Develop Organization and Human Resources
1. Establish Security Standard

Preparation of Security Standard for the entire system life-cycle

<table>
<thead>
<tr>
<th>Basic Concept</th>
<th>Requirement Definition</th>
<th>Design / Development</th>
<th>Deployment / Operation</th>
</tr>
</thead>
</table>
| • Making security guideline  
  • Continuous budget for security  
  • Organization for security  
  • etc... | • Considering security in requirements  
  • Designing system based on security standard like IEC62443  
  • Building Incident Response process  
  • etc... | • Secure coding  
  • Redundant system  
  • Fuzz testing, Penetration testing  
  • Utilizing a test-bed  
  • etc... | • Operation scheme based on CSMS  
  • Review of normal operation, i.e., use of external medias  
  • Clarifying Incident Response process  
  • Regular assets inventories  
  • etc... |
2. Defense in Depth

• **Direction**
  – **Existing Factory: Minimizing downtime**
    • Early anomaly detection and rapid recovery from damages without changing existing facilities
  – **New Factory: Prevention**
    • Protection without impacting on availability and performance

• **3 Steps approach**
  1. Prevent incoming threats and attacks
  2. **Existing Factory: Anomaly detection without system changes. New Factory: Prevent facilities and devices from threats**
  3. Quick recovery
Solution Example: New Factory

- **TippingPoint™ Threat Protection System**
  - Next generation IPS against vulnerability attack

- **Deep Discovery™ Inspector**
  - Early anomaly detection
  - Threats’ visibility

- **Trend Micro Safe Lock™**
  - Lockdown AV software without using pattern file

- **Trend Micro Portable Security 2™**
  - USB shaped AV scanning tool without software installation

- **Trend Micro USB Security™**
  - Secure USB flash drive
  - *Available in specific regions only

- **Trend Micro Deep Security™**
  - Next generation server security solution

- **Trend Micro IoT Security**
  - Security software for IoT devices

---

*Available in specific regions only*
Customer Case: Nissin Electric Co., Ltd

A Japanese, Kyoto-based electrical equipment company. The company is a member of the Sumitomo Group and a partner of Sumitomo Electric Industries. As of 2015, Nissin Electric has 24 subsidiaries located in Japan, China, Taiwan, Korea, Thailand, Vietnam, India, U.S.A. and Spain.

Trend Micro Safe Lock achieved a stable operation of power supervisory control system that supports factories and community infrastructure

Before

- Increased malware infection risks due to SCADA connected to office network and the use of USB memory stick
- Need a solution of very little impact on the system for operational availability

After

- TMSL achieved to avoid unexpected performance down and the risk of system shutdown caused by general virus scanning and signature updating
- TMPS provides safe product delivery by pre-shipment malware inspection for SCADA
- TMUSB prevents from bringing malware into system

Solution

- Trend Micro Safe Lock
- Portable Security
- USB Security
3. Develop Organization and Human Resources

Utilize knowledge and experiences of IT security for factory security
Establish a cooperative structure of resource development and central management

**Executives**
Implement cooperation, integration and resource exchange as company policy

**OT division**
- Understand environment changes
- Increase of security awareness
- Utilize knowledge of IT division

**IT division**
- Study about Industrial Control Systems
- Understand the different security requirements from IT system
- Manage entire company security
Market Leadership Position

**Trend Micro** delivers the **most cloud security controls (16 of 21)** of all evaluated vendors.

- IDC, Securing the Server Compute Evolution: Hybrid Cloud Has Transformed the Datacenter, January 2017 #US41867116

**Gartner**

- **The market leader** in server security for 7 straight years
- **Recommended** Breach Detection System for 4 straight years, and **Recommended** Next-generation IPS

**Gartner**

- **Leader** in Gartner Magic Quadrant for Intrusion Detection and Prevention Systems, January 2018
- Trend Micro delivers the most cloud security controls (16 of 21) of all evaluated vendors.

**Gartner**

- **Named a Leader Once Again** in the Gartner Magic Quadrant for Endpoint Protection Platforms, Jan 2018

**AV-TEST**

- **#1** in protection and performance

- [https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html](https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html)
- [av-test.org](http://av-test.org) (Jan 2014 to Dec 2017)
Enables your business and reduces risk

Automates security & streamlines incident response

Simplifies compliance and enables tool consolidation
Thank you!