Security issues and solutions for next generation Factories

25th Apr 2017

Yuki Ueda
Product Marketing Manager
Trend Micro Incorporated.
28 years focused on security software
Headquartered in Japan, Tokyo Exchange Nikkei Index (4704)
Annual sales over $1B US
Customers include 45 of top 50 global corporations
5500+ employees in over 50 countries

500k commercial customers &
155M endpoints protected
• Threats
  – Security incidents in Japan
  – Ransomware in ICS / SCADA
  – Issues and Challenges

• Solutions
  – Security solution for ICS/SCADA
  – Customer cases
  – Demonstration
Security incidents in Japan

Source: Trend Micro Incorporated, Sep, '14
Internet survey to 218 persons involved in managing industrial control system of FA and PA system.

*1 Have you ever encountered malware infection on an industrial control systems which you manage? (N=218)

*2 As result, have you ever encountered production-stop? If you have, let us know its period (N=92)

- Infected, 42.2%
- No infection, 47.2%
- Unknown, 10.6%

Malware infection ratio of ICS*1 infected, more than 6 days in some case.
Energy Sector

Malware infection on a monitoring terminal of energy control system via USB Storage

No social impact, but took 1 day for recovery.
Manufacturing Sector

Malware infection on a control terminal in the FA system

Production stopped 5 days,
Delay of delivery

Source: Internet survey, Trend Micro Incorporated.
Ransomware in ICS / SCADA

• Factory infected via USB Storage/OA NW in Japan*1

• Loss 100KUSD, production stop half month, in Brazil*2

• Temporary blackout by infection via USB Storage, in Brazil*3

*R2, 3: http://www.darkreading.com/endpoint/ransomware-rising-on-the-plant-floor/d/d-id/1327870
Issues and Challenges

- Insufficient countermeasure
  - Vendor’s responsibility?
    - Vendor’s responsibility
    - Difficulty of applying security patch
- Vulnerability
  - Legacy OS
  - IT dept has no responsibility for facilities, but field dept.
  - Signature file is not updated
• Existing facilities
  Anomaly detection and quick recovery without changing structures

• New facilities
  Protect facilities without impacting system performance
Steps of Layered protection

1. Intrusion prevention
   - Network, USB Storage, Maintenance Work PC

2. Anomaly detection
   - Machine tools, control terminals, etc.

3. Quick recovery
   - backup, malware cleanup tool
Deployment example

- **Office**
- **Office PC**
- **Office Server**
- **Factory**
- **MES OPC Client**
- **OPC Server**
- **DMZ File Server**
- **Supplier Integrator**
- **HMI**
- **EWS**
- **PLC/DCS**
- **Remote maintenance**
- **Maintenance Service**

**TippingPoint™ Threat Protection System**

**Deep Discovery™ Inspector**

**Trend Micro Portable Security 2™**

**Safe Lock™**

**Trend Micro Deep Security™**

**Trend Micro USB Security™**
<table>
<thead>
<tr>
<th>Customer Cases</th>
<th>Industry Target System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Manufacturing</td>
</tr>
<tr>
<td></td>
<td>Energy</td>
</tr>
<tr>
<td></td>
<td>Water</td>
</tr>
<tr>
<td></td>
<td>Gas</td>
</tr>
<tr>
<td></td>
<td>Transportation</td>
</tr>
<tr>
<td></td>
<td>Retail</td>
</tr>
<tr>
<td></td>
<td>Finance</td>
</tr>
<tr>
<td></td>
<td>Medical</td>
</tr>
</tbody>
</table>

Case details:
Demonstration: Attack & Defense on FA System

- USB malware infection causes operation-stop

- Attacker compromises HMI and displays ransomware-like dialog
Wrap-up

• Many incidents occurred in Japan.

• ICS specific challenges

• Different approach for each facilities with layered protection