Security issues and solutions for next generation Factories

25th Apr 2017

Yuki Ueda
Product Marketing Manager
Trend Micro Incorporated.

About Trend Micro

- 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

Enterprise

Midsize Business

Small Business

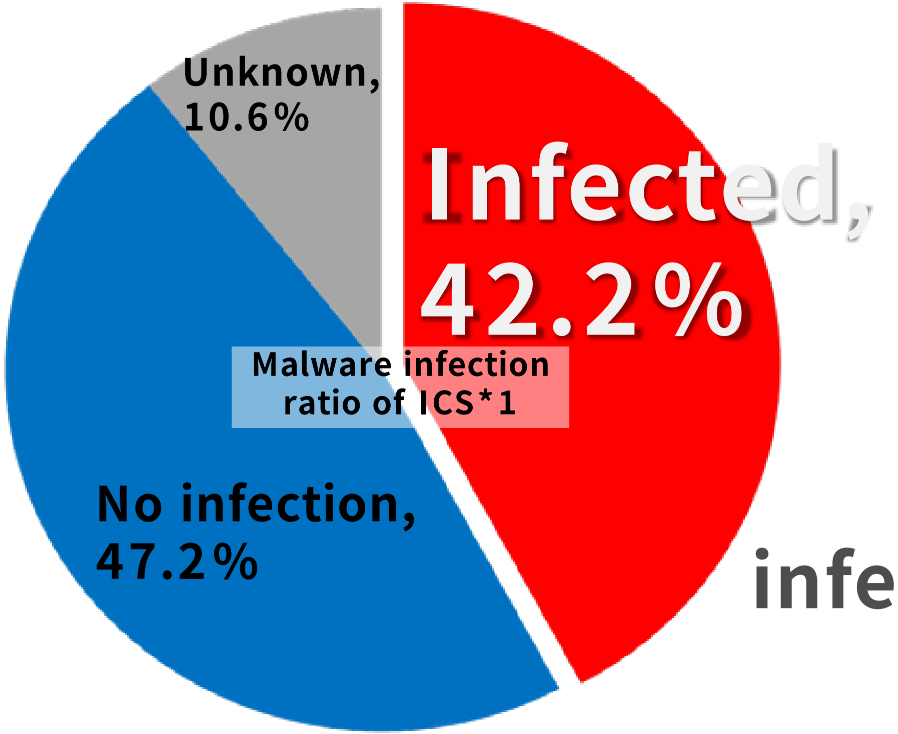
Consumers

Agenda

- Threats
  - Security incidents in Japan
  - Ransomware in ICS / SCADA
  - Issues and Challenges
- Solutions
  - Security solution for ICS/SCADA
  - Customer cases
  - Demonstration

Threats

Security incidents in Japan



55.4%*2

infected factory stopped

More than 6 days in some case

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 mange? (N=218)**

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

Security incidents in Japan

Energy Sector

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

No social impact, but took 1 day for recovery.

Source:
Internet survey, Trend Micro Incorporated.

Security incidents in Japan

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

Ransomware is now a real threat for 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]

Source
*1 : Trend Micro Incorporated.
*2, 3: http://www.darkreading.com/endpoint/ransomware-rising-on-the-plant-floor/d/d-id/1327870

Issues and Challenges

Insufficient countermeasure

- Mindset
  - Vendor's responsibility?
  - Closed system is safe?
- Vulnerability
  - Legacy OS
  - Difficulty of applying security patch
- Limitation
  - Software installation is prohibited
  - Signature file is not updated
  - IT dept has no responsibility for facilities, but field dept.

Solutions

Approach concept

- 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

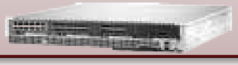
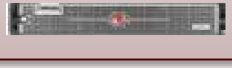
2. Anomaly detection

   Machine tools, control terminals, etc…

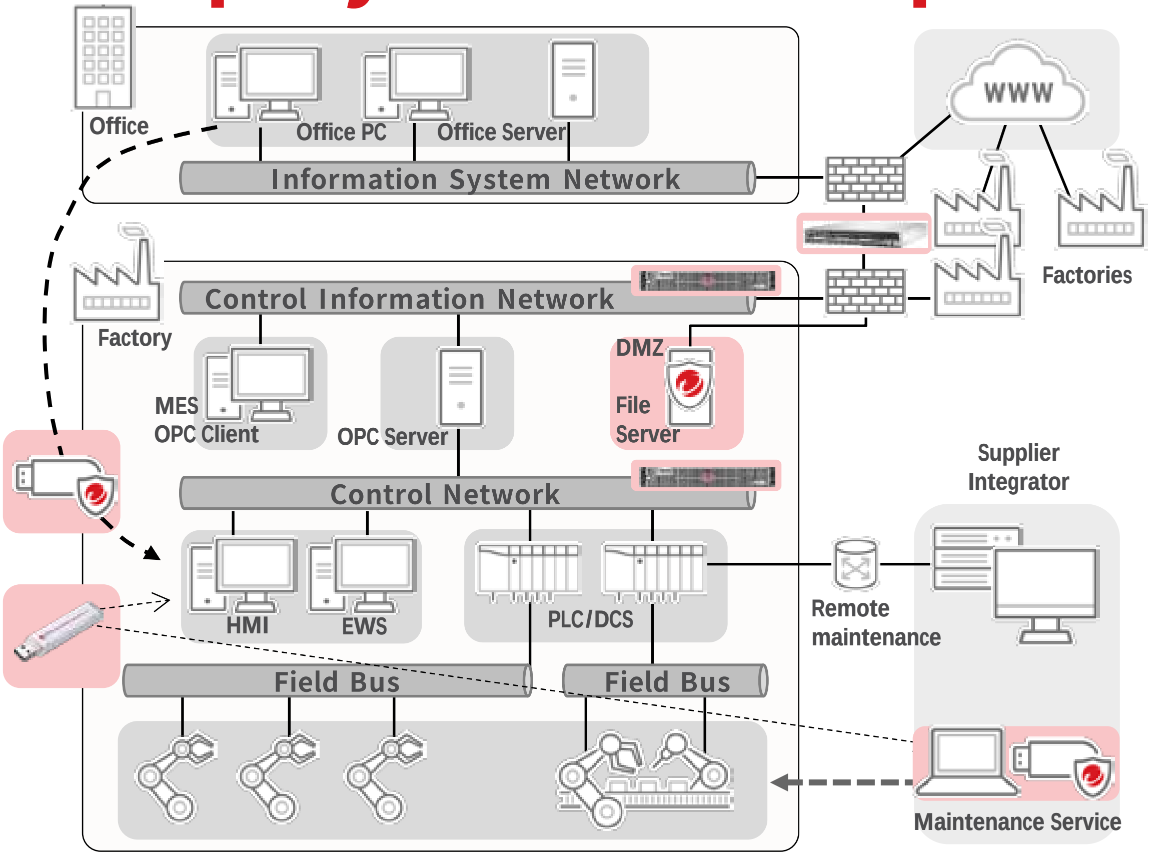
3. Quick recovery

   backup, malware cleanup tool

Ref: Security solution for ICS / SCADA

	Gateway/ Network	Server / Client PC		External Device
		Plant DMZ / Control Information Network	Control Network	
		Non Mission-Critical General Purpose	Mission Critical Specific purpose	
Prevention	TippingPoint Threat Protection System™ “Next generation Intrusion Prevention System” 	Trend Micro Deep Security™ “Comprehensive, modular protection for servers, desktops and laptops”	Trend Micro Safe Lock™ “Lockdown security software for fixed-function devices”	Trend Micro USB Security™ “Protect USB Storage”
Detection	Deep Discovery™ Inspector “Network Visibility, early anomaly detection” 		Trend Micro Portable Security 2™ “Malware scan / cleanup tool without software installation” 	
Cleanup	N/A			

Deployment example –Existing facilities-



TippingPoint™ Threat Protection System
Next generation
Intrusion Prevention System

Deep Discovery™ Inspector
Network visualization,
early anomaly detection

Trend Micro Portable Security 2™
Malware scan / cleanup tool
without software installation

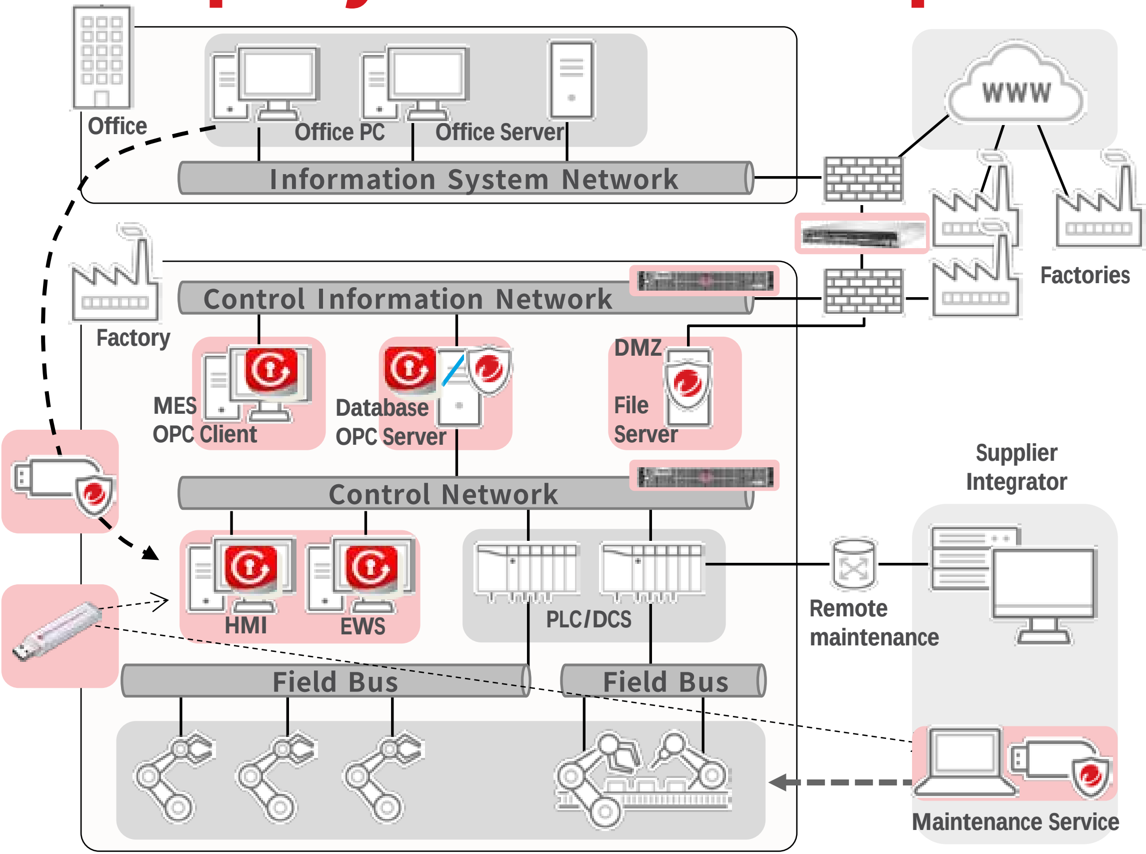
Trend Micro Safe Lock™
System lockdown software for
fixed-function devices

Trend Micro Deep Security™
Comprehensive, modular protection
for servers, desktops and laptops

Trend Micro USB Security™
Protect USB Storage

TREND MICRO

Deployment example –New facilities-



TippingPoint™ Threat Protection System

Next generation
Intrusion Prevention System

Deep Discovery™ Inspector

Network visualization,
early anomaly detection

Trend Micro Portable Security 2™

Malware scan / cleanup tool
without software installation

Trend Micro Safe Lock™

System lockdown software for
fixed-function devices

Trend Micro Deep Security™

Comprehensive, modular protection
for servers, desktops and laptops

Trend Micro USB Security™

Protect USB Storage

Customer Cases inc. critical infrastructures

SUZUKI Perfecting the Art of Electronics ALPS YOKOGAWA NISSIN ELECTRIC

Industry	Target System
Manufacturing	Production System of FA/PA
Energy	Power Plant System
Water	Water System
Gas	LPG Filling System
Transportation	Railway Control System, Air traffic Control System
Retail	POS system
Finance	Core Banking System, ATM, Trading System
Medical	PACS, eHR

Case details:

Suzuki : http://www.trendmicro.co.jp/jp/business/case-study/articles/20150210013658.html
ALPS : http://www.trendmicro.co.jp/jp/business/case-study/articles/20161227085203.html
Yokogawa: http://www.trendmicro.co.jp/jp/business/case-study/articles/20150213084224.html
Nissin Electric: http://www.trendmicro.co.jp/jp/business/case-study/articles/20160609010854.html

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

Thank you.

TREND MICRO