Industry 4.0 and Attacks on Manufacturing Networks, Myths or Reality?

Fyodor Yarochkin
Senior Threat Researcher
Trend Micro
@fygrave

Bakuei Matsukawa
Senior Threat Researcher
Trend Micro
Question: a two years old malware can cause over 80 mil loss in one day.

Is this a myth or reality?
What really had happened?

Virus outbreak caused almost NT 2.6 billion (US 84.28 mil) of loss <3/08/2018>
Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plants

Renault-Nissan said on Monday that output had returned to normal at nearly all its plants, after a global cyber attack caused widespread disruption including stoppages at several of the auto alliance’s sites.

Renault and its Japanese partner are the only major car manufacturers so far to have

Cyber Attack At Honda Stops Production After WannaCry Worm Strikes

Peter Lyon Contributor

I focus on all things to do with cars.
Targeted Attacks in Manufacturing Networks: a case study

Duck Test: if it walks like a duck, is it really a duck 😊
PlugX on Manufacturing Network

PlugX is a remote access trojan (RAT) first identified in 2012 that targeted government institutions. It is similar to the Poison Ivy malware, allowing remote users to perform data theft or take control of the affected systems without permission or authorization. PlugX is distributed through email attachments in spearphishing campaigns, mainly targeting specific businesses and organizations.
PlugX and Ransomware: incident highlights

- 2017/09/10 02:00:42 AM: Identified execution of C:\RECYCLER\demo.exe
- The binary was deployed through IIS web service process w3wp.exe
- Dropped BKDR_PLUGX.ZTEG: iusb3mon.dll sha1: cedd4391f03b00b319e93b6a7f8fd69fbc6059e5
- 2017/09/10 02:00:40 attacker uploaded HKTL_MIMIKATZ: C:\RECYCLER\m32.exe
- Spread laterally
- This Victim: a manufacturing enterprise in China
Our indicators match the ransomware incident?

- An incident was reported by tencent (https://s.tencent.com/research/report/461.html) on a different victim
- The hacker **extorted the victimized company** in the message on the desktop

"We are not a ransomware that spreads automatically, we are professional hacker organization that specifically targets enterprises" .. Give us 9.5 BTC!
PlugX for ransom is not a single instance. Attacker Targets Manufacturing Industry

- We identified more targets in Taiwan and China

<table>
<thead>
<tr>
<th>Date</th>
<th>Detection Path</th>
<th>Accessed by</th>
<th>Detection</th>
<th>Industry</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/09/2017 18:03</td>
<td>C:\RECYCLER\demo.exe</td>
<td>C:\WINDOWS\system32\inetsrv\w3wp.exe</td>
<td>BKDR_PLUGX.ZTEG</td>
<td>Manufacturing</td>
<td>CN</td>
</tr>
<tr>
<td>20/09/2017 08:34</td>
<td>C:\PerfLogs\demo.exe</td>
<td>C:\Windows\explorer.exe</td>
<td>BKDR_PLUGX.ZTEG</td>
<td>Manufacturing</td>
<td>CN</td>
</tr>
<tr>
<td>09/10/2018 01:39</td>
<td>C:\root\80.exe</td>
<td>C:\WINDOWS\system32\inetsrv\w3wp.exe</td>
<td>BKDR_PLUGX.DUKRX</td>
<td>Manufacturing</td>
<td>TW</td>
</tr>
</tbody>
</table>
Not a Single Instance: Targeted ransomware and mining campaigns

Dediki = Dedicated servers
Strange things in Manufacturing Networks

another case
Equation tools weaponized to distribute coin miner
Snapshot of activity in the affected infrastructures
The exploitation stage happens at the spike

CVE-2017-0143
And then.. Lateral movement

EQUATION TOOLS
Use of equation tools
And deploying coin-miner
As well as remote access tools

BACKDOOR ZEGOST
Examine the victims

Important Observation

- All of the victim machines of this campaign were on INTERNAL network. Possibly protected by a firewall, Intrusion Detection System and so on.
- This did not stop the opportunistic attackers from breaking in.
Advanced Targeted Attack Tools Found Being Used to Distribute Cryptocurrency Miners

Posted on: June 13, 2019 at 5:09 am    Posted in: Malware    Author: Trend Micro

by Cedric Pernet, Vladimir Kropotov, and Fyodor Yarochkin

Regular cybercriminals appear to be taking a page from targeted attack actors’ playbooks — or rather, toolkits — to maximize their profits from illicit activities like cryptojacking.

One of the differences between regular cybercrime and targeted attacks is intent: The former will almost always have immediate financial gain as its main motivation while the latter will have other goals, for example, intellectual property theft. Furthermore, the mindsets of the threat actors can be very different. Regular cybercriminals will typically need to think of how they can compromise as many individual devices as possible (for example, to deliver ransomware, coin miners, or banking trojans) while targeted attack threat actors will need to plan how to infiltrate and gain full access to corporate networks and remain as discreet as possible.

APT tools For Coin mining and Ransom
Modern Manufacturing networks

Let's understand the environment and its weaknesses
What is Industry 4.0?

1700s
Mechanical manufacturing
Steam-powered machines replaced human labor

1800s
Mass production
Electric-powered machines aided the production of goods in massive quantities

1900s
IT automation
IT enabled the use of geographically disparate systems, reducing production cost

2000s
Cyber-physical system use
Technologies like ML/AI enabled automated information sharing and even decision making
## Is Industry 4.0 a Buzzword? – No

<table>
<thead>
<tr>
<th>Country</th>
<th>Strategy</th>
<th>Issue Date</th>
</tr>
</thead>
</table>
| China   | Made in China 2025  
中国製造2025重点領域技術路線図 | May-15 |
| Germany | Industrie 4.0 | Nov-11 |
| India   | Make in India  
Digital India | Sep-14 |
| Japan   | Connected Industries  
Society 5.0 | Mar-17 |
| Russia  | 4.0RU | Jul-17 |
| US      | Industrial Internet Consortium  
Manufacturing USA | Mar-14 |
Convergence of IT, OT and IP

Information Technology + Operational Technology + Intellectual Property = Industry 4.0

Convergence of traditional IT, OT equipment and IP assets
So how Manufacturing networks differ from regular IT?

What are the problems?
So how Manufacturing OT networks differ from regular IT?

Intellectual Property

OT

Malicious insider

Gains access to

Unwitting employee

Infects

Compromises

Steals

Pivots into

Compromises

Steals

Infects

IT

Threat actor

Gains access to
Availability
## Use of Windows XP in Manufacturing

<table>
<thead>
<tr>
<th>OS Type</th>
<th>Manufacturing Industry</th>
<th>Other industries</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>60.2%</td>
<td>61.0%</td>
<td>-0.8%</td>
</tr>
<tr>
<td>Windows 10</td>
<td>28.9%</td>
<td>29.4%</td>
<td>-0.5%</td>
</tr>
<tr>
<td>Windows 8.1</td>
<td>5.3%</td>
<td>5.8%</td>
<td>-0.5%</td>
</tr>
<tr>
<td>Windows XP</td>
<td>4.4%</td>
<td>2.5%</td>
<td>+1.9%</td>
</tr>
<tr>
<td>Windows XP 64-bit</td>
<td>0.5%</td>
<td>0.3%</td>
<td>+0.2%</td>
</tr>
<tr>
<td>Windows 8</td>
<td>0.4%</td>
<td>0.7%</td>
<td>-0.3%</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>0.2%</td>
<td>0.2%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>0.1%</td>
<td>0.1%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

Percentage point differences between distribution of operating systems in Manufacturing and other industries based on Trend Micro telemetry data for the period from July to December 2018.
# Prevalence of Downad in Manufacturing

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Manufacturing Industry</th>
<th>Other industries</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan</td>
<td>39.3%</td>
<td>40.6%</td>
<td>-1.3%</td>
</tr>
<tr>
<td>PUA</td>
<td>14.7%</td>
<td>15.3%</td>
<td>-0.6%</td>
</tr>
<tr>
<td><strong>Worm</strong></td>
<td><strong>9.9%</strong></td>
<td><strong>8.3%</strong></td>
<td><strong>+1.6%</strong></td>
</tr>
<tr>
<td>Hacking tool</td>
<td>7.5%</td>
<td>6.7%</td>
<td>+0.8%</td>
</tr>
<tr>
<td>Cryptocurrency miner</td>
<td>4.0%</td>
<td>3.6%</td>
<td>+0.4%</td>
</tr>
<tr>
<td>Adware</td>
<td>3.6%</td>
<td>4.4%</td>
<td>-0.8%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malware Family</th>
<th>Manufacturing Industry</th>
<th>Other industries</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>WannaCry</td>
<td>3.3%</td>
<td>3.2%</td>
<td>+0.1%</td>
</tr>
<tr>
<td><strong>Downad</strong></td>
<td><strong>2.9%</strong></td>
<td><strong>1.2%</strong></td>
<td><strong>+1.7%</strong></td>
</tr>
<tr>
<td>Coinminer</td>
<td>2.0%</td>
<td>0.5%</td>
<td>+1.5%</td>
</tr>
<tr>
<td>MalXMR</td>
<td>1.8%</td>
<td>1.2%</td>
<td>+0.6%</td>
</tr>
</tbody>
</table>

Percentage point differences between distribution of malware types and families in Manufacturing and other industries based on Trend Micro Telemetry for the period from July to December 2018.
Malicious Autorun.inf detections

Detections of Autorun.inf across industries based on Trend Micro Telemetry for the period from July to December 2018

- Manufacturing: 25.77%
- Government: 13.49%
- Education: 12.73%
- Healthcare: 11.68%
- Technology: 5.63%
- Energy: 4.66%
- Oil and gas: 2.80%
- Utilities: 2.44%
- Banking: 2.07%
- Retail: 2.05%
- Others: 16.68%
Data exchange via USB between IT and OT
Threats and Risks to Intellectual Property In Manufacturing industry
Unintentional leaks due to poor configuration
## Malicious CAD files

<table>
<thead>
<tr>
<th>ACM_SHENZ.A</th>
<th>ACM_MEDRE.AA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Create a user with admin privileges</td>
<td>• Send PST file of Microsoft Outlook to a predefined email address</td>
</tr>
<tr>
<td>• Create writable network shares</td>
<td>• Send an opened CAD (DWG) file to a predefined email address</td>
</tr>
<tr>
<td>• Open ports for SMB with vulnerabilities</td>
<td></td>
</tr>
</tbody>
</table>

CAD files can be weaponized for espionage
Use of older version of Microsoft Office

Microsoft Word 97 macro (W97M) detections by Microsoft Office version

Comparison of versions of Microsoft Office, which includes Microsoft Word, from the National Cyber Security Centre
Distribution of Confidential information

Stolen Confidential Documents can be distributed in public

止まらぬ日本企業の文書流出 中国サイトに186社分（日本経済新聞・2018年3月1日）
https://www.nikkei.com/article/DGXMO2756453001032018CR8000/

インターネットを活用した新しい侵害形態

第2回情報技術情報防衛シンポジウム
「中国における営業秘密漏えいの実態、及びこれに対する効果的な対応方策」
(IP FORWARD・2015年1月27日)
Distribution of leaked CAD files

Sites showing leaked CAD files pertaining to a popular smartphone

Stolen CAD data also can be distributed in public
Counterfeit products issue

$250 billion a year damage worldwide


One of major crimes for INTERPOL


Counterfeit is a serious issue for Manufacturing companies

UN News

Illicit goods - the issues

There is a clear link between illicit trade and other types of crime, such as human trafficking, drug trafficking, corruption, bribery and money laundering. Illicit trade damages the global economy and harms public health worldwide. All regions of the world and all industry sectors are affected.

Counterfeit becomes “Supercopy”

The issue can be more serious in the era of Industry 4.0

Piln !pect Market  China “Supercopy” ha 
http://www.nhk.or.jp/gendai/articles/3857/1.html
Other Threats and Risks to exposed OT systems
Exposed ICSs
Underground Activities Related to Manufacturing industry
SCADA 0days dealt on the Underground

Vulnerabilities in scada
The topic in the "Buy / Sell / Exchange" section was created by 4t4k4, Jun 30, 2015.

4t4k4
Newbie

Good day to all. interested in 0-day vulnerabilities in the SCADA system. Ready to pay well to anyone who can help JID: sp1d3r@exploit.im
PLC password crackers sold online on the underground
Klassny
Member
Registered: 2014-10-12
Posts: 15
PM

Intellectual Property, Assets, Confidential, Industrial Spionage

Dear EVO

I'm looking for anything that falls that category. If you work on a big name, multinational, bank, tech firm or whatever. I'm buying:

- Blueprints, CAD, CAM Files
- Source Code, Software
- Confidential Documents
- Custom sensible information, competitive advantage
- Finance Algos, Black Boxes

We discuss revenue details on PM. If you hate your employer or you think you worth more, talk to me.
Rent-A-Hacker

Experienced hacker offering his services! (Illegal) Hacking and social engineering is my business since I was 16 years old, never had a real job so I had the time to get really good at hacking and I made a good amount of money last ++20 years. I have worked for other people before, now I am also offering my services for everyone with enough cash here.

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small job, for example: Email and Facebook hacking, installing trojans, small DDOS</td>
<td>250 EUR = 0.029 $</td>
</tr>
<tr>
<td>Medium-large job, ruining people, espionage, website hacking, DDOS for big websites</td>
<td>500 EUR = 0.059 $</td>
</tr>
<tr>
<td>Large job which takes a few days or multiple smaller jobs, DDOS for protected sites</td>
<td>900 EUR = 0.106 $</td>
</tr>
<tr>
<td>UPGRADE: INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If I need longer this will get refunded. Only buy this together with one of the other options.</td>
<td>200 EUR = 0.024 $</td>
</tr>
</tbody>
</table>
Industrial equipment purchase request

Greetings friends, I need a man who will drive the equipment I need is not expensive, who will make cheaper, so I will work.

**immediately write to drive away the shkolodrocherov.**

I will work only through the guarantor, at my expense, the guarantor until I receive the machines I need.

machine tools on 3-15T.p.
only about 3-5 stations, the situation will show, I can take the staff even at your own address for your convenience. further will work with a proven person on a permanent, telephones and small electronics, buying up both on order and without, if there are such people here, write to the cart.

dog CobaltDron
Shodan Shop with Industrial Section

With Google search, we determine that we are invited to log in by the `ewON`, with the login account `adm` and the password `adm`.

**industrial VPN router**
Examining the root causes and best practices

And answer the question “WHY”
THE ROOT CAUSE

Where is the ..
Interconnection between IT and OT
Equipment Lifecycle

3-5 years **IT** vs 26-34 years **OT**
Stay UP TO DATE

Windows XP is 17 years old
Threat Modeling: identify Information flows

- Think like a hacker: How could Intellectual Property Information be exfiltrated from my network?
- What are the information flow channels?
- What are controls that allow me to prevent this?
Defense in Depth

- Defense in Depth is extremely critical in context of Industry 4.0
- Do not assume that the OT networks are isolated
- Stay up to date
- Segregate and Segment
- Enforce controls
Security Recommendations For Manufacturing
Basic Security Principles

- Restrict user access and permissions
- Enforce domain or subnetwork restrictions
- Disable directory listing
- Remove or disable unnecessary services
Security Recommendations for Manufacturing

- Technological Measures
  - How to do
- Human Operations
  - Human Factors
- Security Policy
  - What to do
Security Recommendations for Manufacturing

- **Technological Measures**
  - How to do

- **Human Operations**
  - Human Factors

- **Security Policy**
  - What to do

- • Accounting and Prioritization of Assets
- • Making Security a Requirement
- • IEC 62443 Compliance
Security Recommendations for Manufacturing

How to do

- User Education
- Cooperation between IT and OT

Human Operations

- Accounting and Prioritization of Assets
- Making Security a Requirement
- IEC 62443 Compliance

Technological Measures

Human Factors

What to do

Security Policy
Security Recommendations for Manufacturing

- **Technological Measures**
  - Application of Appropriate Protection

- **Human Operations**
  - User Education
  - Cooperation between IT and OT

- **Security Policy**
  - Accounting and Prioritization of Assets
  - Making Security a Requirement
  - IEC 62443 Compliance
Conclusions and Final Remarks
# Myth Buster

<table>
<thead>
<tr>
<th>Assumption</th>
<th>Myth?</th>
</tr>
</thead>
<tbody>
<tr>
<td>OT network is closed and isolated</td>
<td>Myth</td>
</tr>
<tr>
<td>Windows XP is still in-production in the manufacturing</td>
<td>Reality</td>
</tr>
<tr>
<td>Mostly targeted by APT groups</td>
<td>Myth</td>
</tr>
<tr>
<td>Industry 4.0 is a buzz word</td>
<td>Myth</td>
</tr>
<tr>
<td>CAD files are safe</td>
<td>Myth</td>
</tr>
<tr>
<td>Industrial equipment may be operated by outsiders</td>
<td>Reality</td>
</tr>
<tr>
<td>Customized PLC password crackers</td>
<td>Reality</td>
</tr>
<tr>
<td>Old Worms and Infections still active in OT Networks</td>
<td>Reality</td>
</tr>
<tr>
<td>Blueprints, CAM files are targeted only by APT groups</td>
<td>Myth</td>
</tr>
</tbody>
</table>
So what is a real Myth?

Attacks on Manufacturing Networks are always sophisticated
RSA Conference 2019
Asia Pacific & Japan

Thank you!

fyodor_yarochkin@trendmicro.com
bakuei_matsukawa@trendmicro.com