

RSA® Conference 2019 Asia Pacific & Japan

Singapore | 16–18 July | Marina Bay Sands



SESSION ID: CMI-W09

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

#RSAC

RSA® Conference 2019 Asia Pacific & Japan

**Question: a two years old malware
can cause over 80 mil loss in one day.**

Is this a myth or reality?



Taiwan Semiconductor

Latest Politics Cross-Straight Economics Entertainment & Sports

Virus outbreak caused almost NT 2.6 billion (US 84.28 mil) of loss

<3/08/2018>

What really had happened?

TSMC Spokesperson

Lora Ho
Senior Vice President &
Tel: 886-3-5054602

Taipei, Nov. 16 (CNA) Taiwan Semiconductor Manufacturing Co. (TSMC), the world's largest contract chipmaker, reported Thursday that it lost NT\$2.6 billion (US\$84.28 million) in the

TSMC Acting Spokesperson

Elizabeth Sun
Senior Director, TSMC Corporate Communications D
Tel: 886-3-5682085
Email: elizabeth_sun@tsmc.com

Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plants



Laurence Frost and Naomi Tajitsu, Reuters May 15, 2017,

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

Forbes

[Billionaires](#)[Innovation](#)[Leadership](#)[Money](#)[Consumer](#)

9,396 views | Jun 22, 2017, 05:00am

Cyber Attack At Honda Stops Production After WannaCry Worm Strikes



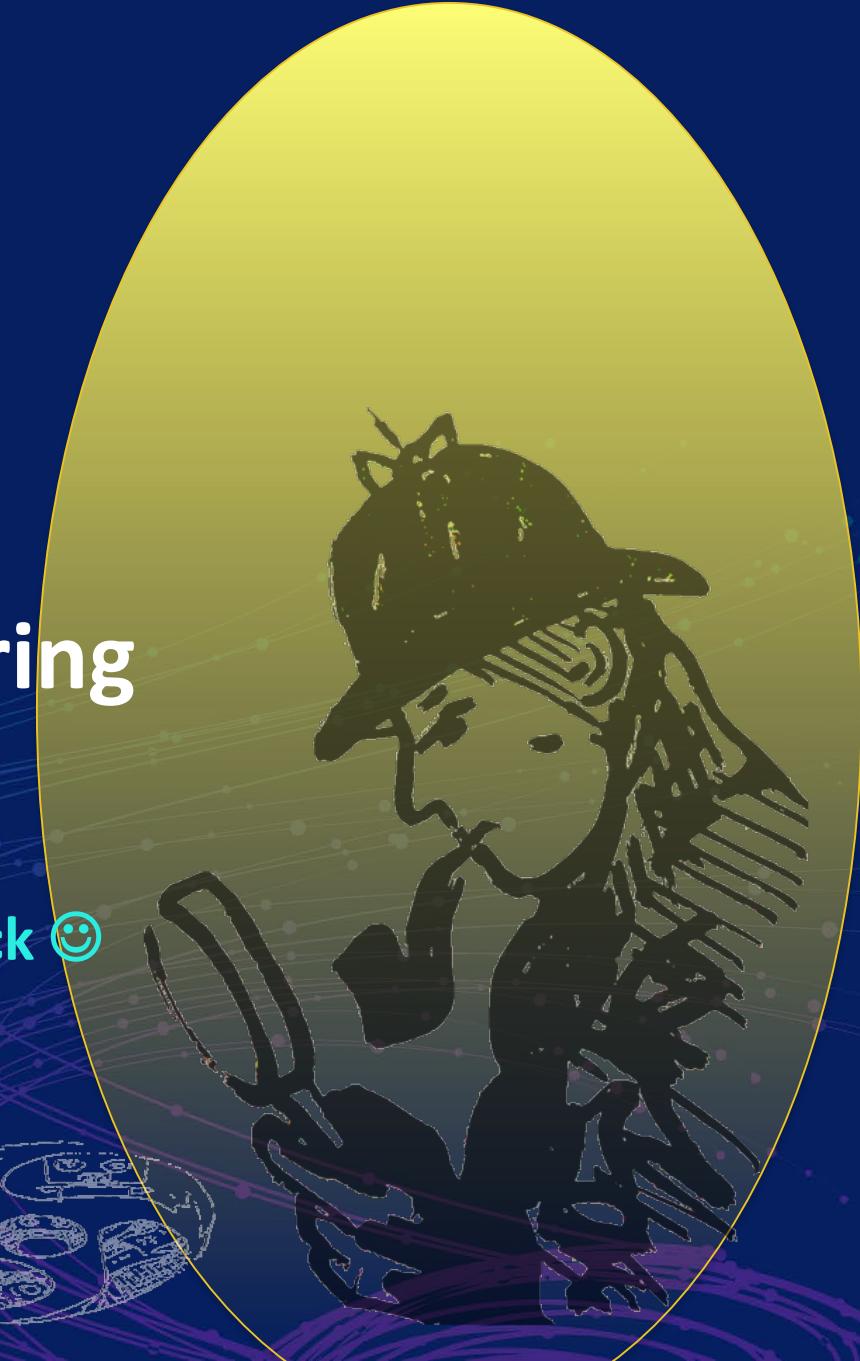
Peter Lyon Contributor

I focus on all things to do with cars.

RSA® Conference 2019 Asia Pacific & Japan

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

The screenshot shows a web browser window with the URL <https://www.cyber.nj.gov/threat-profiles/trojan-variants/plugx>. The page is from the NJCCIC (New Jersey Cybersecurity and Communications Integration Center) website. The header includes the NJCCIC logo, a navigation menu with links to HOME, REPORT, ABOUT, THREAT CENTER, RESOURCES, and JOIN, and standard browser icons for favoriting, sharing, and saving. The main content area features a large title "PlugX" and a subtitle "APRIL 12, 2017 • TROJAN VARIANTS". Below this, a detailed description of the PlugX malware is provided.

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

Date	Detection Path	Accessed by	Detection	Industry	Country
09/09/2017 18:03	C:\RECYCLER\demo.exe	C:\WINDOWS\system32\inetsrv\w3wp.exe	BKDR_PLUGX.ZTEG	Manufacturing	CN
20/09/2017 08:34	C:\PerfLogs\demo.exe	C:\Windows\explorer.exe	BKDR_PLUGX.ZTEG	Manufacturing	CN
09/10/2018 01:39	C:\root\80.exe	C:\WINDOWS\system32\inetsrv\w3wp.exe	BKDR_PLUGX.DUKRX	Manufacturing	TW

Not a Single Instance: Targeted ransomware and mining campaigns

Checked Sell Dediki under vb * c, miner, locker, poker, etc. | Sample by country | Low prices | Dedicated servers | DediTe.com

defender71 · 01/25/2019 · nl brut dediki rdp dedik to buy dedik to buy



defender71

New user

check in: 01/25/2019
Messages: one
Sympathy: 0
Points: one

01/25/2019

On sale there are various Dedik under WB * in, poker, miner, locker, etc.

Sort by country:

RU / UA - 130 rub.

USA / Canada - 150 rubles.

Europe - 140 rubles.

China - 80 rubles. (Often taken under the cryptors and miners)

(Germany, France, Spain, Italy, England, Japan, Netherlands, Czech Republic, Poland)

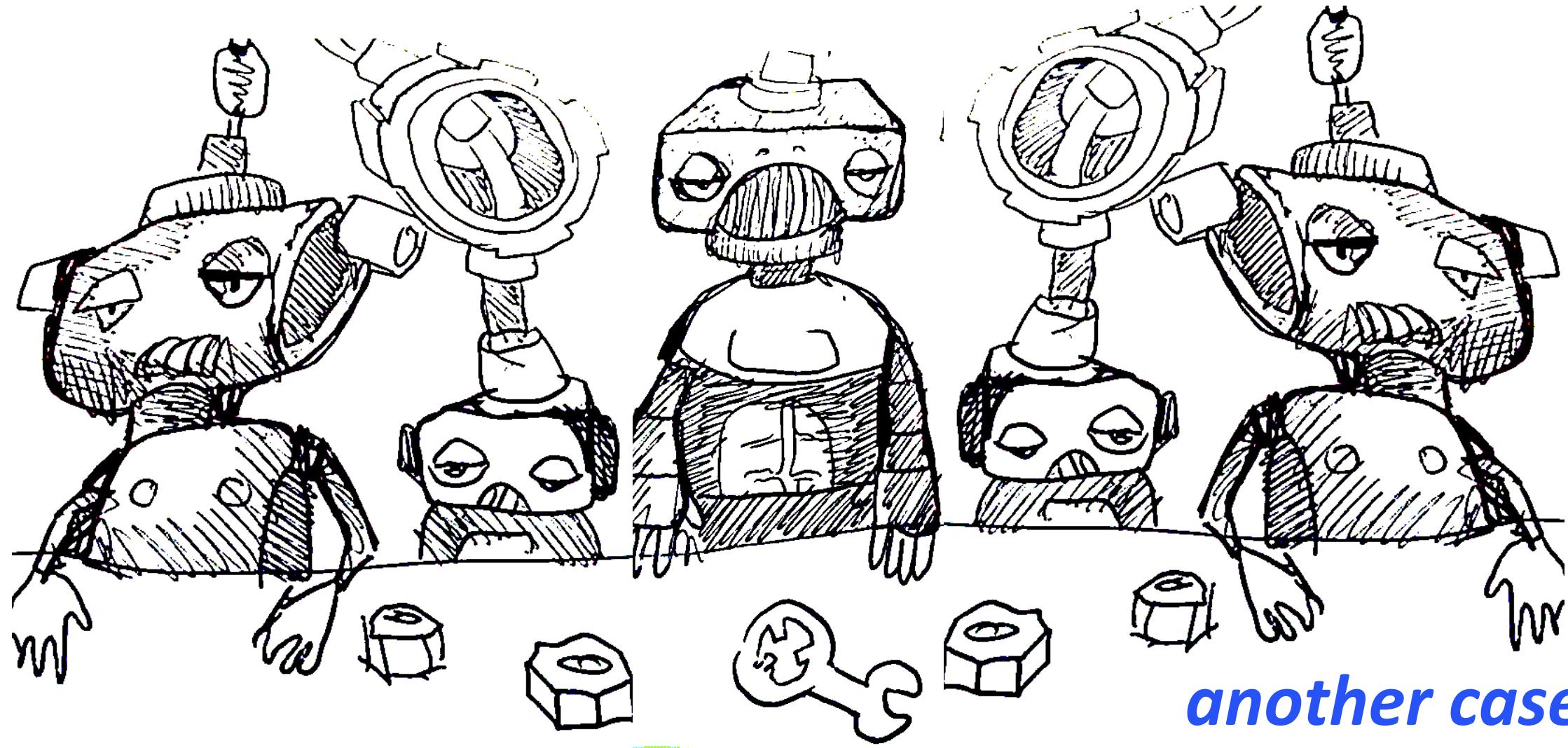
There are also many other countries, find out the presence of certain countries by contacts!

Regular customers discounts!

Contacts:

Dediki =
Dedicated
servers

Strange things in Manufacturing Networks



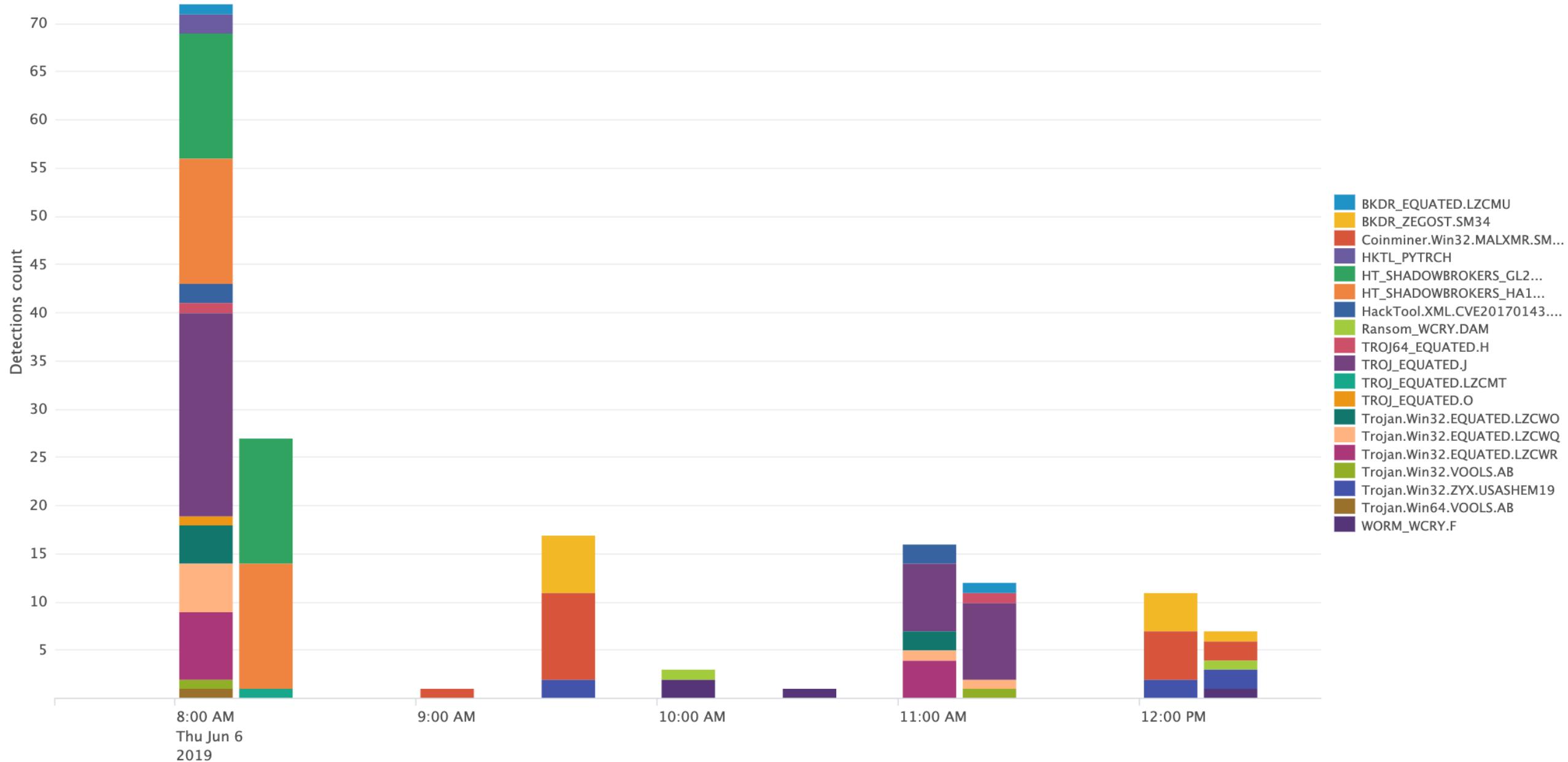
another case

Equation tools weaponized to distribute coin miner

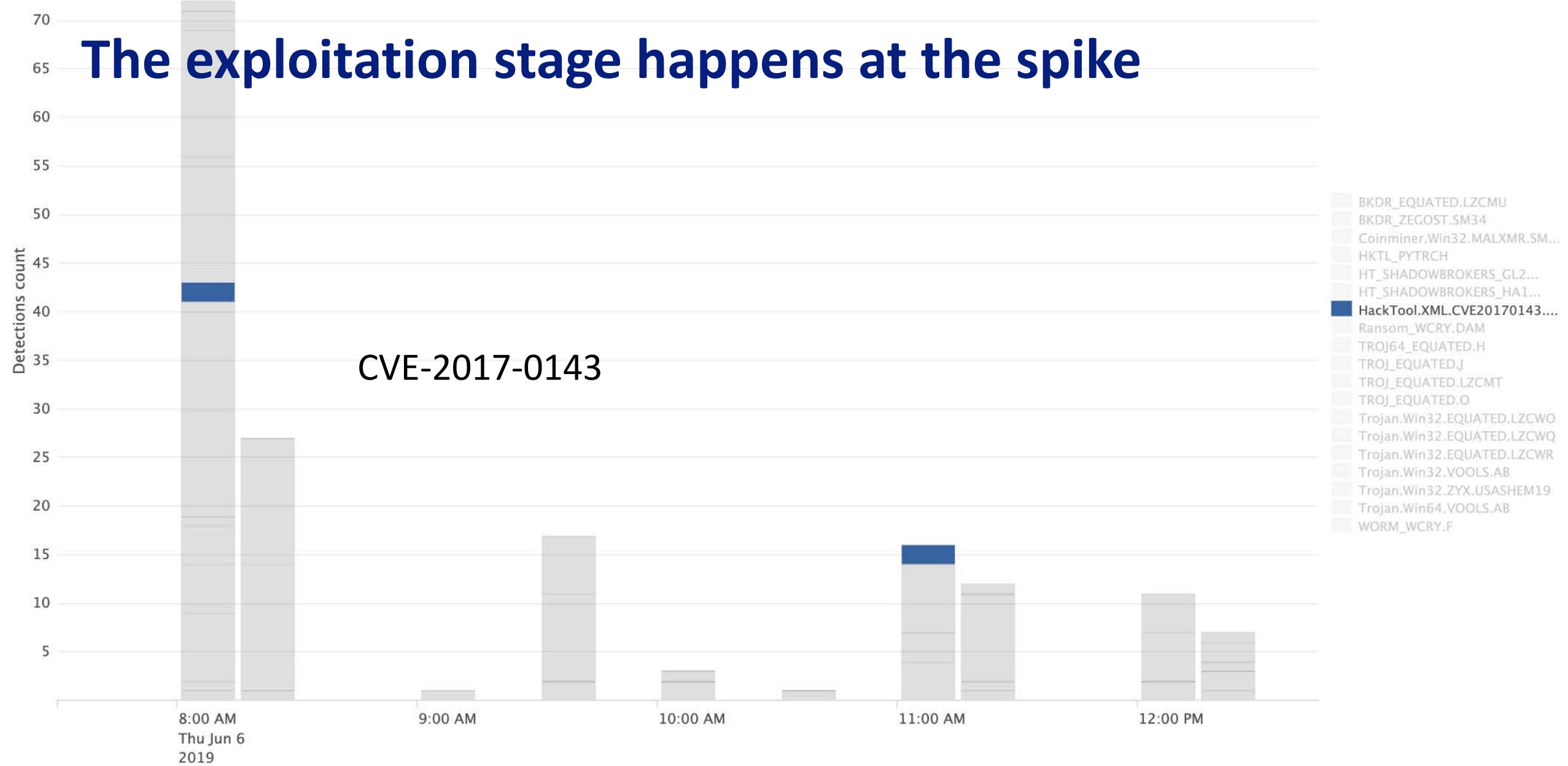
The screenshot shows a GitHub repository page for 'misterch0c / shadowbroker'. The repository title is 'misterch0c / shadowbroker'. Below the title, there are navigation links for 'Code' (highlighted in orange), 'Issues 7', 'Pull requests 1', 'Projects 0', 'Security', and 'Insights'. A main heading reads 'The Shadow Brokers "Lost In Translation" leak'. Below this, there are summary statistics: '24 commits', '1 branch', and '0 releases'. A dropdown menu shows 'Branch: master ▾' and a button for 'New pull request'. Three repository items are listed: 'misterch0c white knight fix', 'oddjob', and 'swift'. The 'swift' item has a note: 'decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...'.

Snapshot of activity in the affected infrastructures

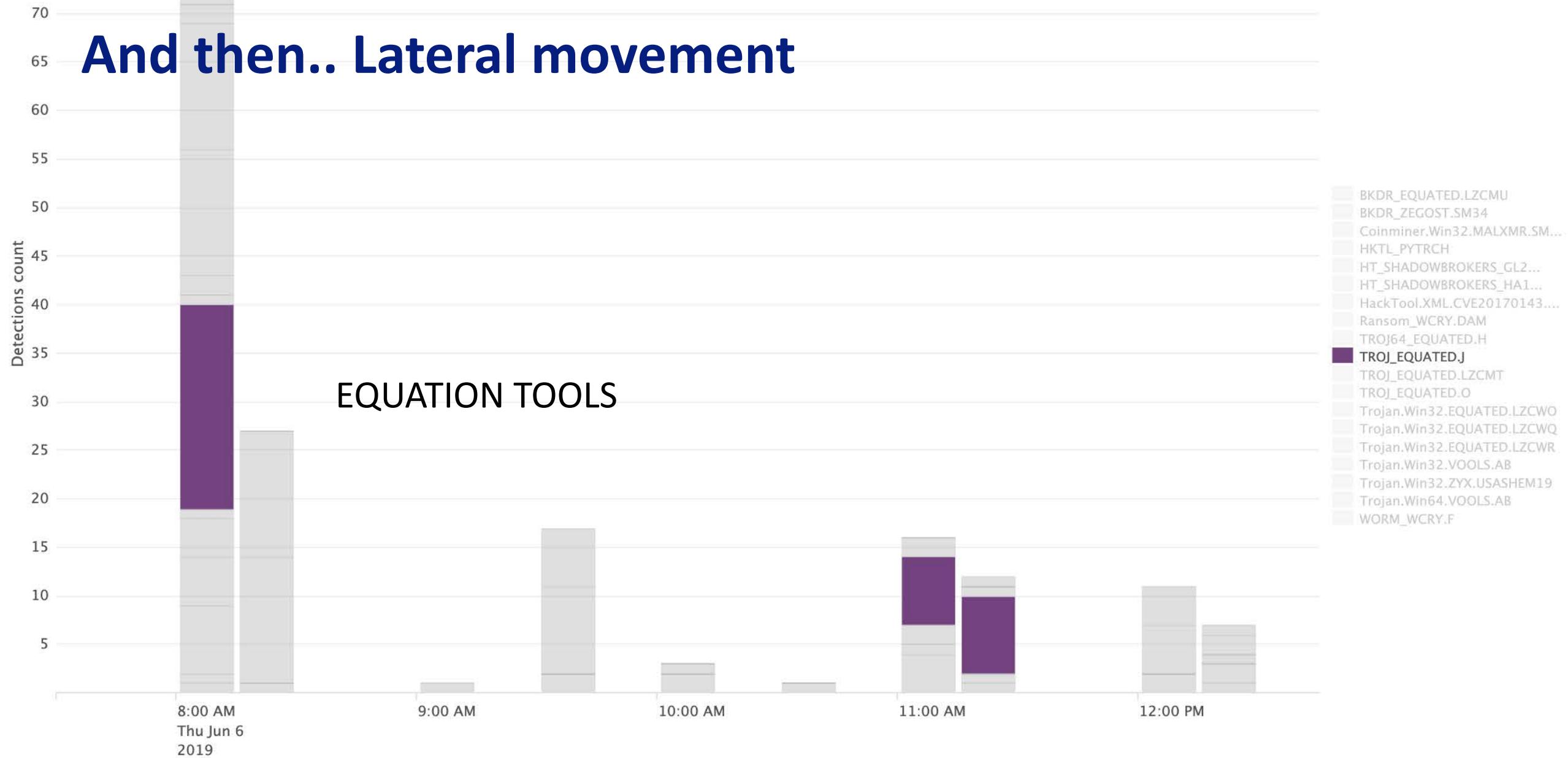




The exploitation stage happens at the spike

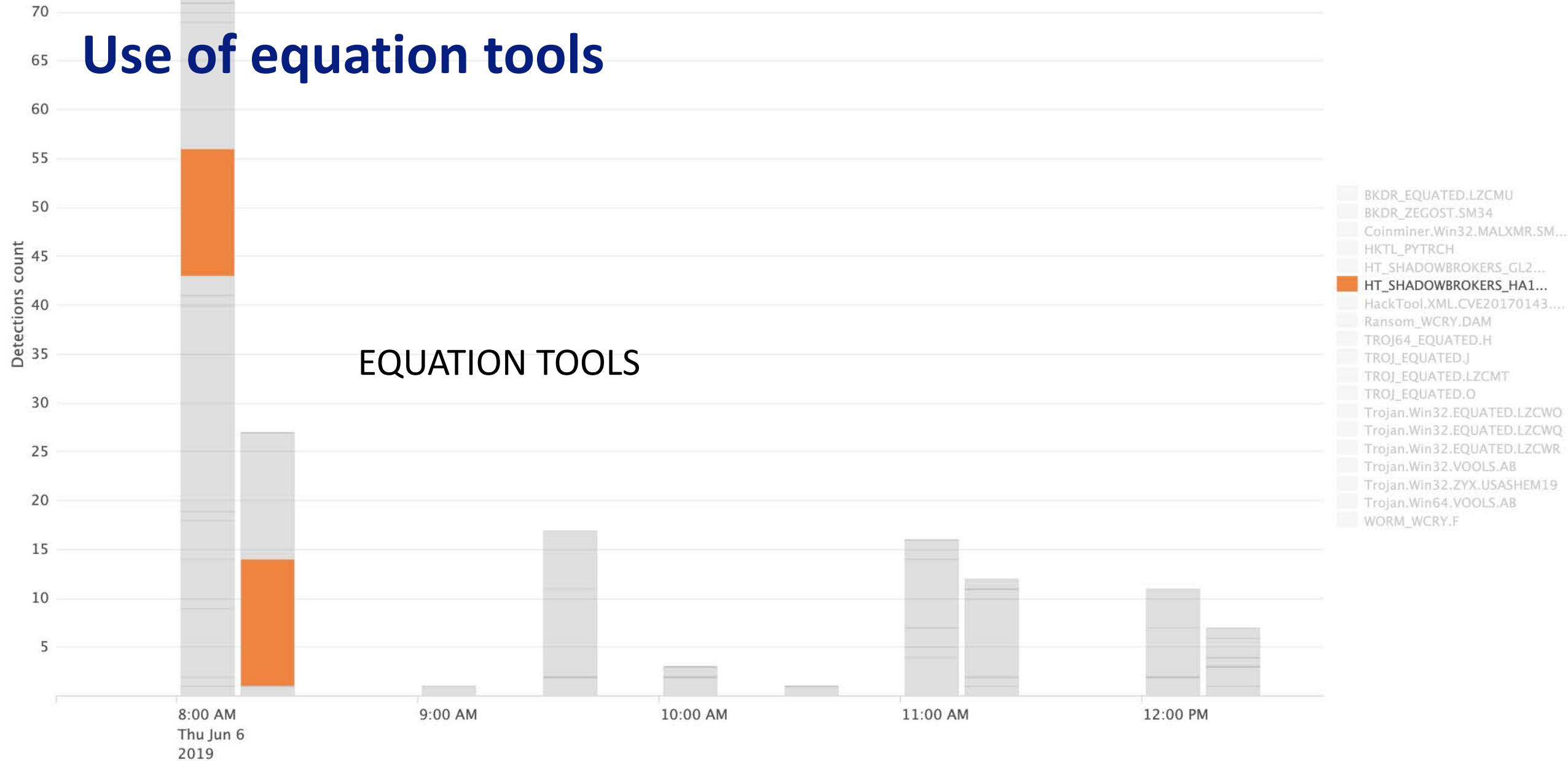


And then.. Lateral movement



8:00 AM
Thu Jun 6
2019

Use of equation tools

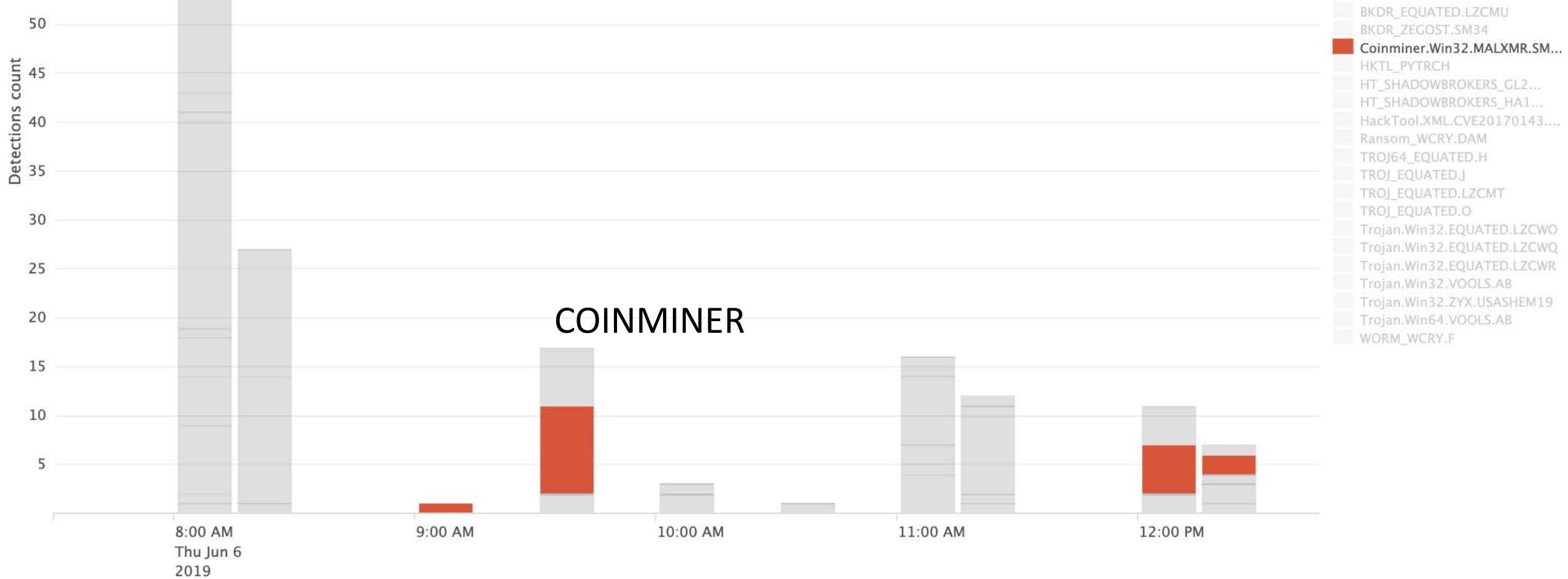


EQUATION TOOLS

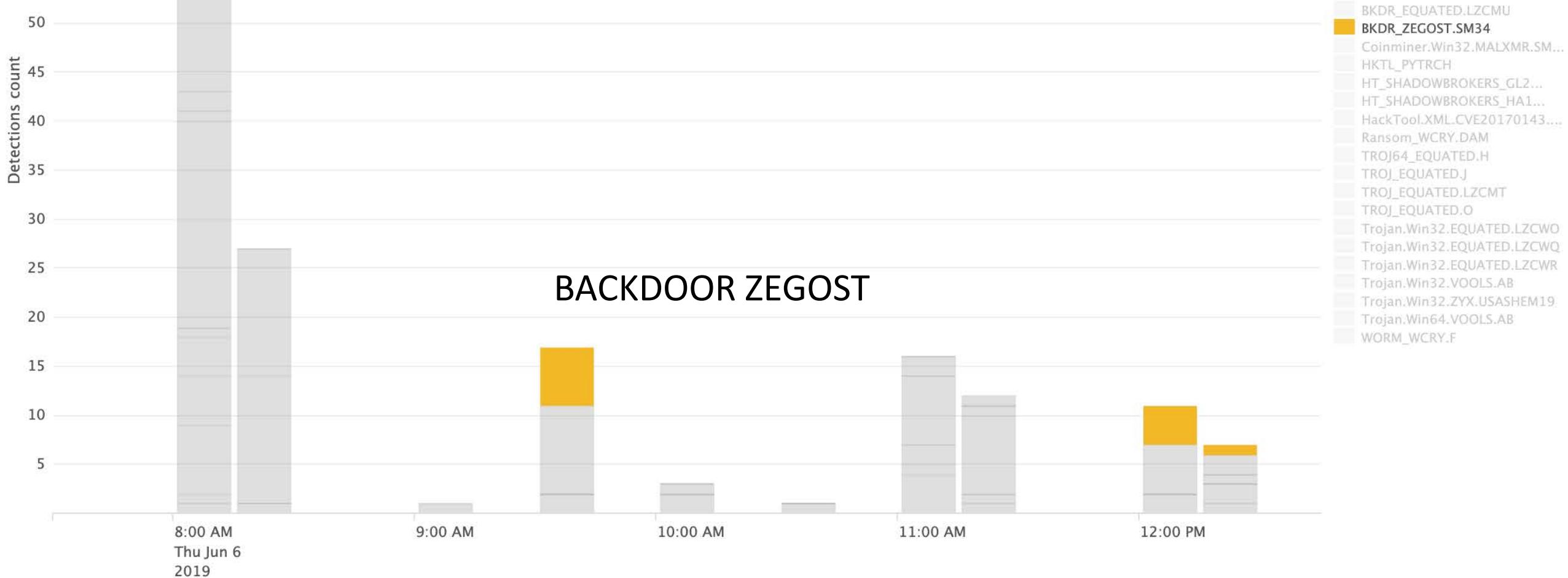
8:00 AM
Thu Jun 6
2019

- BKDR_EQUATED.LZCMU
- BKDR_ZEGOST.SM34
- Coinminer.Win32.MALXMR.SM...
- HKTL_PYTRCH
- HT_SHADOWBROKERS_GL2...
- HT_SHADOWBROKERS_HA1...
- HackTool.XML.CVE20170143...
- Ransom_WCRY.DAM
- TROJ64_EQUATED.H
- TROJ_EQUATED.J
- TROJ_EQUATED.LZCMT
- TROJ_EQUATED.O
- Trojan.Win32.EQUATED.LZCWO
- Trojan.Win32.EQUATED.LZCWQ
- Trojan.Win32.EQUATED.LZCWR
- Trojan.Win32.VOOLS.AB
- Trojan.Win32.ZYX.USASHEM19
- Trojan.Win64.VOOLS.AB
- WORM_WCRY.F

And deploying coin-miner



As well as remote access tools



8:00 AM
Thu Jun 6
2019

BACKDOOR ZEGOST

- BKDR_EQUATED.LZCMU
- BKDR_ZEGOST.SM34**
- Coinminer.Win32.MALXMR.SM...
- HT_PYTRCH
- HT_SHADOWBROKERS_GL2...
- HT_SHADOWBROKERS_HA1...
- HackTool.XML.CVE20170143...
- Ransom_WCRY.DAM
- TROJ64_EQUATED.H
- TROJ_EQUTED.J
- TROJ_EQUTED.LZCMT
- TROJ_EQUTED.O
- Trojan.Win32.EQUATED.LZCWO
- Trojan.Win32.EQUATED.LZCWQ
- Trojan.Win32.EQUATED.LZCWR
- Trojan.Win32.VOOLS.AB
- Trojan.Win32.ZYX.USASHEM19
- Trojan.Win64.VOOLS.AB
- WORM_WCRY.F

Examine the victims

- HRM-3 IBM-PED JA02-SARTHANA K3Server KAVITHA-PC LenaOffice2 MG1795-LAB-AND MG3624-DIV-DHD NetAdmin-DC operation-asst PortEng1-PC PVR150-PC PVR50-PC RCH12001D RD-3 RKH-HISteam RKSSH-Acc-PC rksshfr RKSSH-HR3 RNV-CR-WF SAL-Leslie SAPERPDEV Shashi-HP SVShah-PC SZ-RDNB002 TallyEC-PC Thomas-Win7 VALVE-TESTING1 VENKAT-FIN Win-Marc Win-SolomonPC3 YE-MAINSTORE3 YEQC-DELL YE-SHIPPING5 YUDESIGN-5 YU-STORE-1

YUKEN

■ **PVR 150-Series Single Vane Pumps**

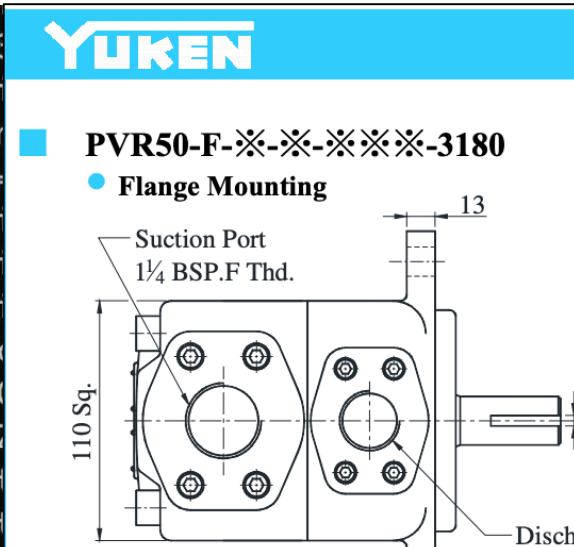
RCH12001 Repair camera head



ZOOM

log.boreye.com,/ipc.html?mac=08:00:27:3F:5A:C4&ip=1.1.2.28&host=SAL-Leslie&tick=30ml?mac=08:00:27:3F:5A:C4&ip=1.1.2.28&host=SAL-Leslie&tick=30ml?mac=08:00:27:3F:5A:C4&ip=1.1.2.48&host=ADM-Vince-Test&tick=30ml?mac=08:00:27:3F:5A:C4&ip=1.1.2.6&host=Goran-NB2&tick=30ml?mac=08:00:27:40:6E:2A&ip=1.1.2.21&host=LenaOffice2&tick=30og.boreye.com,/ipc.html?mac=08:00:27:4F:CA:97&ip=1.1.2.48&host=Win-SolomonPC3&tick=30og.boreye.com,/ipc.html?mac=08:00:27:4F:CA:97&ip=1.1.2.48&host=Win-Marc&tick=30og.boreye.com,/ipc.html?mac=08:00:27:7a:0d:d3&ip=0.0.0.0&host=analyst0-2d1671&tick=30og.boreye.com,/ipc.html?mac=18:66:DA:4E:1C:17&ip=10.20.1.11&host=HFSERVER002&tick=30og.boreye.com,/ipc.html?mac=1A:A3:C4:C4:35:B0&ip=192.168.22.104&host=PortEng1-PC&tick=30og.boreye.com,/ipc.html?mac=2E:93:A2:DC:2D:A5&ip=172.17.0.47_172.17.0.20&host=Salog.boreye.com,/ipc.html?mac=40:61:86:F4:9E:3D&ip=10.129.96.132&host=KAVITHA-PC&tick=30og.boreye.com,/ipc.html?mac=40:61:86:F4:9E:3D&ip=10.129.96.132&host=KAVITHA-PC&tick=30

log.boreye.com,/ipc.html?mac=08:00:27:3F:5A:C4&ip=1.1.2.28&host=SAL-Leslie&tick=30ml?mac=08:00:27:3F:5A:C4&ip=1.1.2.28&host=ADM-Vince-Test&tick=30ml?mac=08:00:27:3F:5A:C4&ip=1.1.2.6&host=Goran-NB2&tick=30ml?mac=08:00:27:40:6E:2A&ip=1.1.2.21&host=LenaOffice2&tick=30og.boreye.com,/ipc.html?mac=08:00:27:4F:CA:97&ip=1.1.2.48&host=Win-SolomonPC3&tick=30og.boreye.com,/ipc.html?mac=08:00:27:4F:CA:97&ip=1.1.2.48&host=Win-Marc&tick=30og.boreye.com,/ipc.html?mac=08:00:27:7a:0d:d3&ip=0.0.0.0&host=analyst0-2d1671&tick=30og.boreye.com,/ipc.html?mac=18:66:DA:4E:1C:17&ip=10.20.1.11&host=HFSERVER002&tick=30og.boreye.com,/ipc.html?mac=1A:A3:C4:C4:35:B0&ip=192.168.22.104&host=PortEng1-PC&tick=30og.boreye.com,/ipc.html?mac=2E:93:A2:DC:2D:A5&ip=172.17.0.47_172.17.0.20&host=Salog.boreye.com,/ipc.html?mac=40:61:86:F4:9E:3D&ip=10.129.96.132&host=KAVITHA-PC&tick=30og.boreye.com,/ipc.html?mac=40:61:86:F4:9E:3D&ip=10.129.96.132&host=KAVITHA-PC&tick=30



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

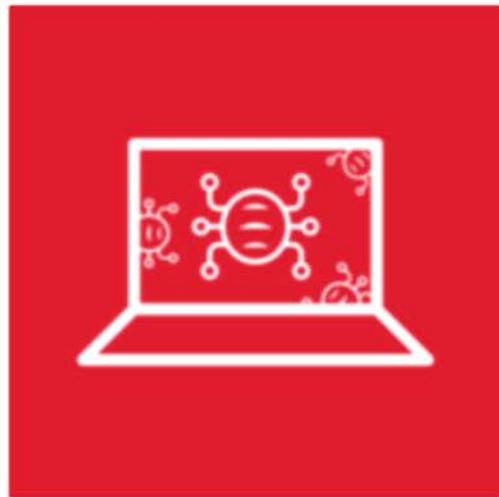
Posted on: [June 13, 2019](#) at 5:09 am Posted in: [Malware](#) Author: [Trend Micro](#)



by *Cedric Pernet, Vladimir Kropotov, and Fyodor Yarochkin*

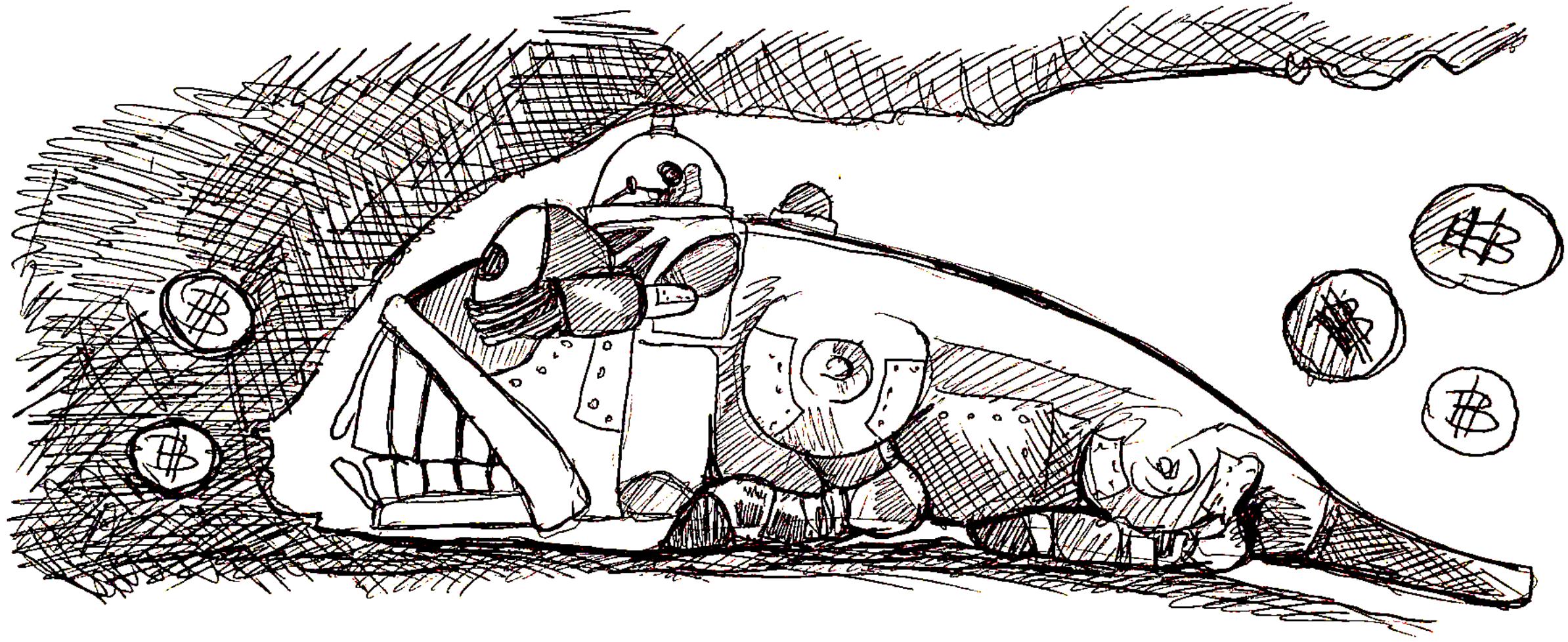
Regular cybercriminals appear to be taking a page from targeted attack actors' playbooks — or rather, toolkits — to maximize their profits from illicit activities like cryptojacking.

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.



<https://blog.trendmicro.com/trendlabs-security-intelligence/advanced-targeted-attack-tools-used-to-distribute-cryptocurrency-miners/>

APT tools For Coin mining and Ransom



RSA® Conference 2019 Asia Pacific & Japan

Modern Manufacturing networks

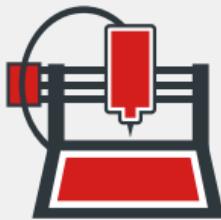
Lets understand the environment and its weaknesses



What is Industry 4.0?

1700s

Mechanical manufacturing

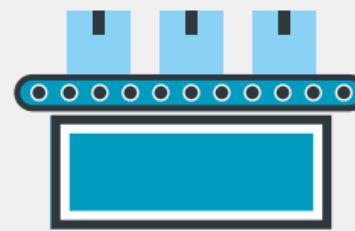


Steam-powered machines replaced human labor

1.0

1800s

Mass production

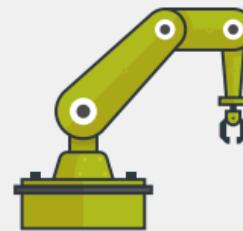


Electric-powered machines aided the production of goods in massive quantities

2.0

1900s

IT automation



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

3.0

2000s

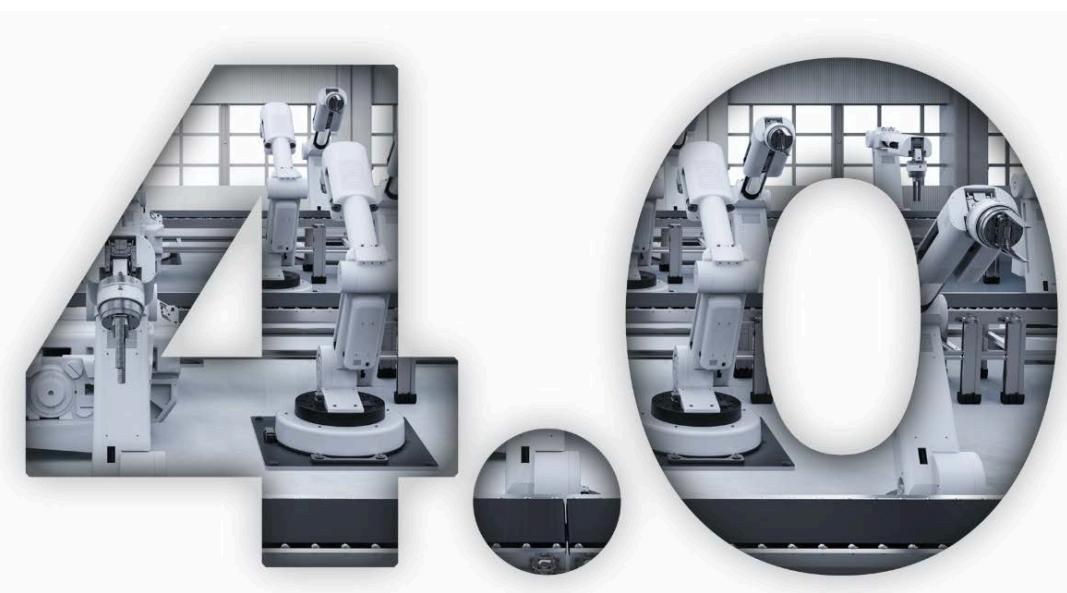
Cyber-physical system use



Technologies like ML/AI enabled automated information sharing and even decision making

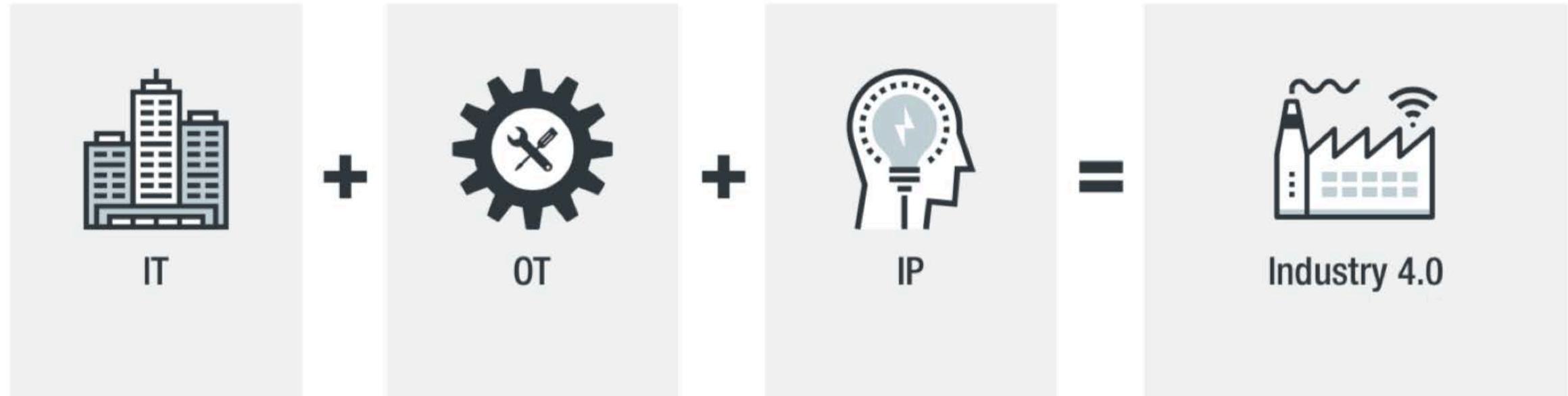
4.0

Is Industry 4.0 a Buzzword? – No



Country	Strategy	Issue Date
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 **T**echnology

Operational **T**echnology

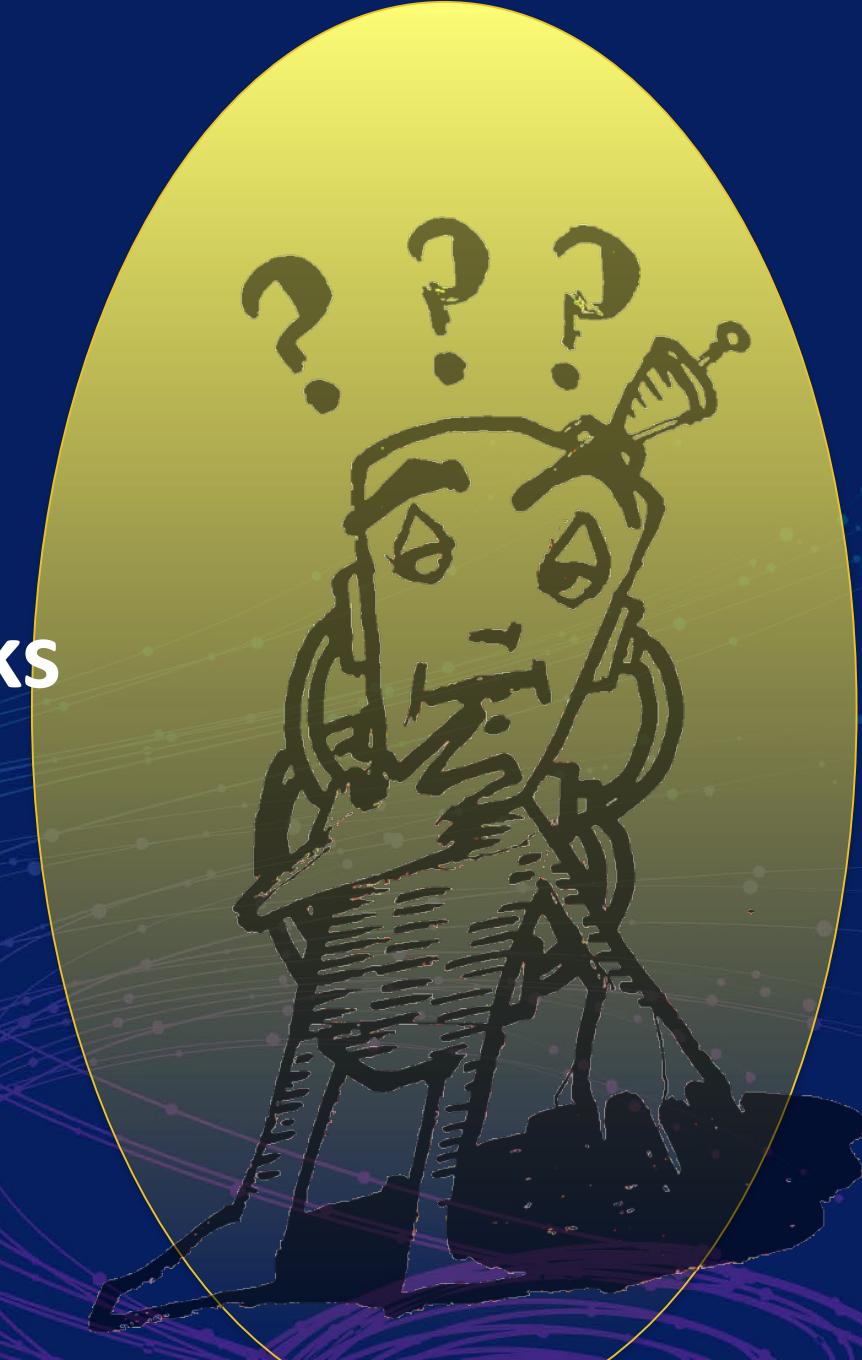
Intellectual **P**roperty

Convergence of traditional **IT**, **OT** equipment and **IP** assets

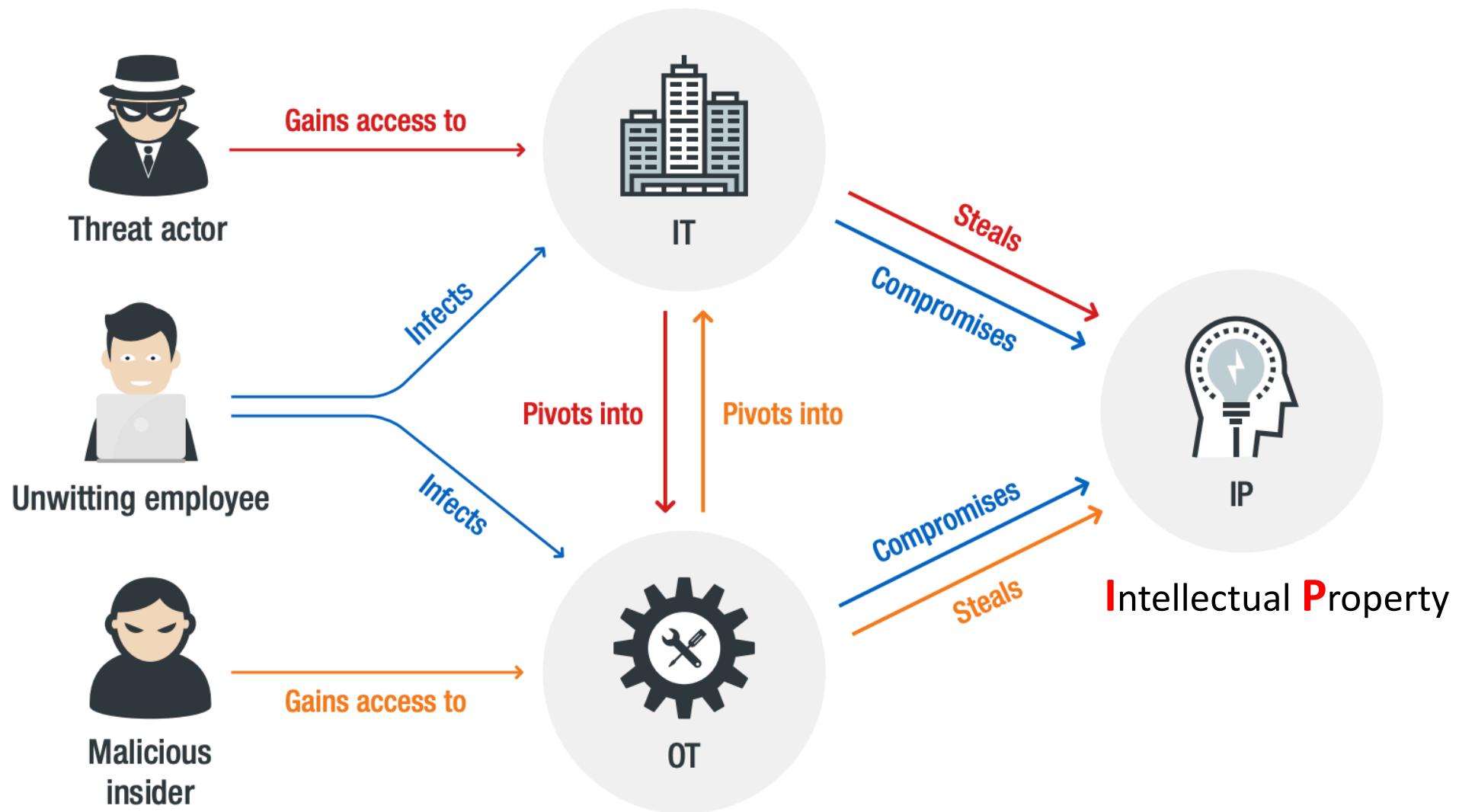
RSA® Conference 2019 Asia Pacific & Japan

So how Manufacturing networks
differ from regular IT?

What are the problems?



So how Manufacturing OT networks differ from regular IT?



Availability



Use of Windows XP in Manufacturing

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

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

Malware Type	Manufacturing Industry	Other industries	Difference
Trojan	39.3%	40.6%	-1.3%
PUA	14.7%	15.3%	-0.6%
Worm	9.9%	8.3%	+1.6%
Hacking tool	7.5%	6.7%	+0.8%
Cryptocurrency miner	4.0%	3.6%	+0.4%
Adware	3.6%	4.4%	-0.8%

Malware Family	Manufacturing Industry	Other industries	Difference
WannaCry	3.3%	3.2%	+0.1%
Downad	2.9%	1.2%	+1.7%
Coinminer	2.0%	0.5%	+1.5%
MalXMR	1.8%	1.2%	+0.6%

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

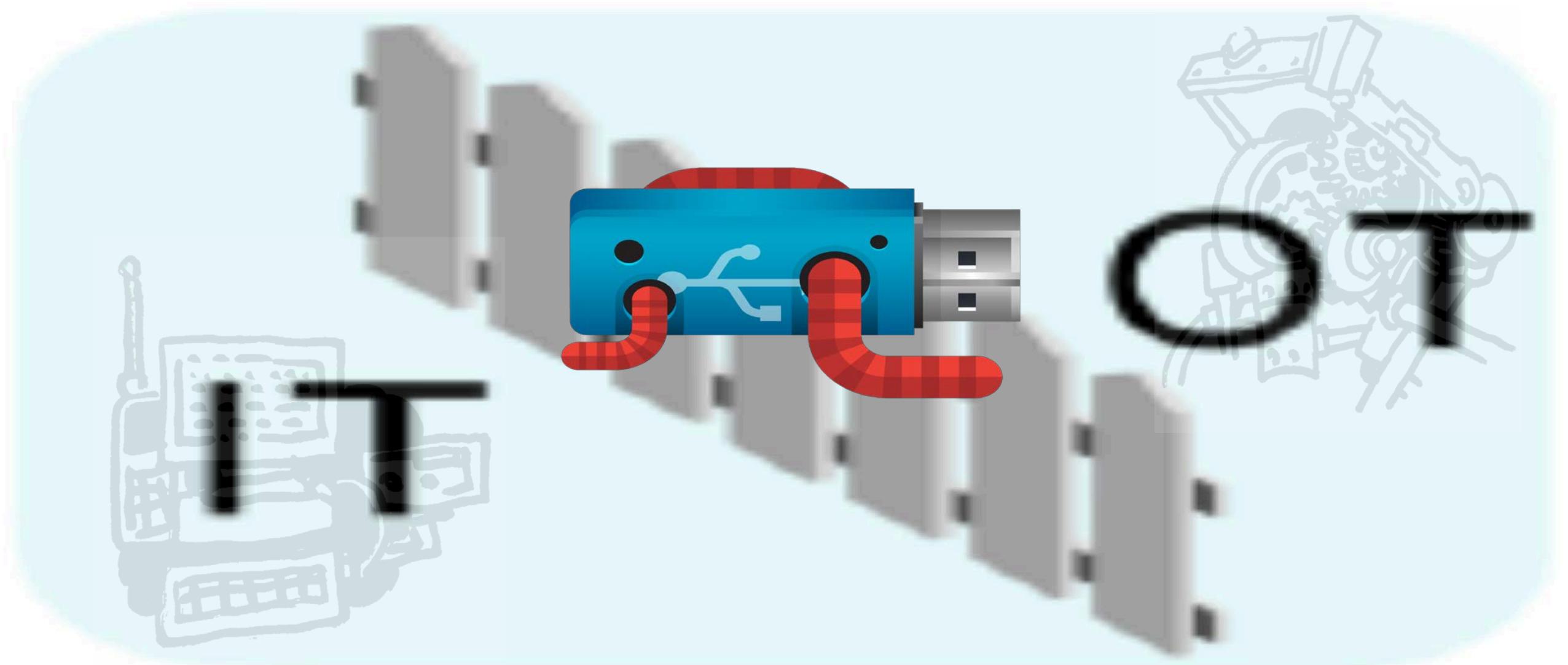
Malicious Autorun.inf detections



- 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%

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

Data exchange via USB between IT and OT

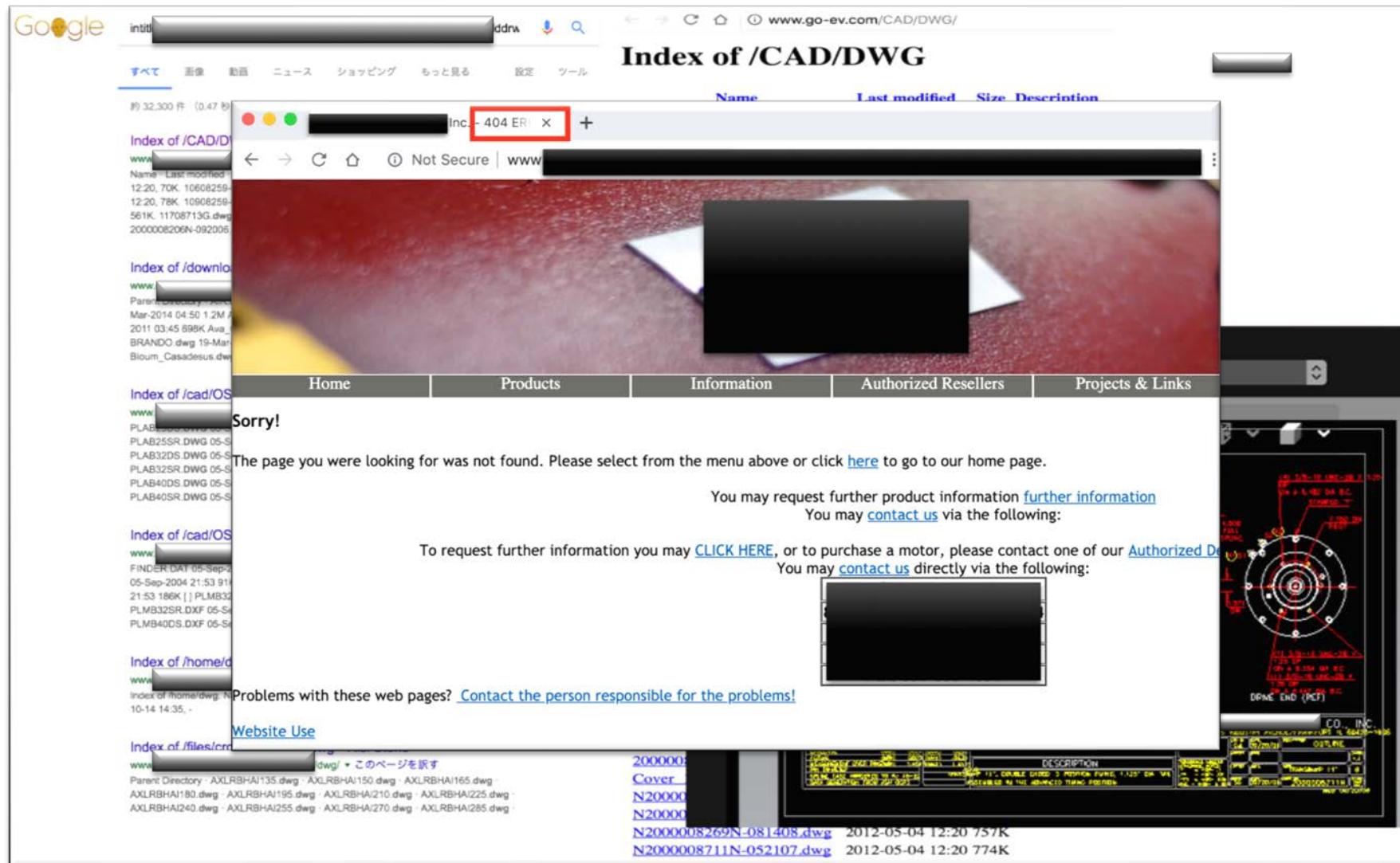


RSA® Conference 2019
Asia Pacific & Japan

Threats and Risks to Intellectual Property In Manufacturing industry



Unintentional leaks due to poor configuration



Malicious CAD files

ACM_SHENZ.A

- Create a user with admin privileges
- Create writable network shares
- Open ports for SMB with vulnerabilities

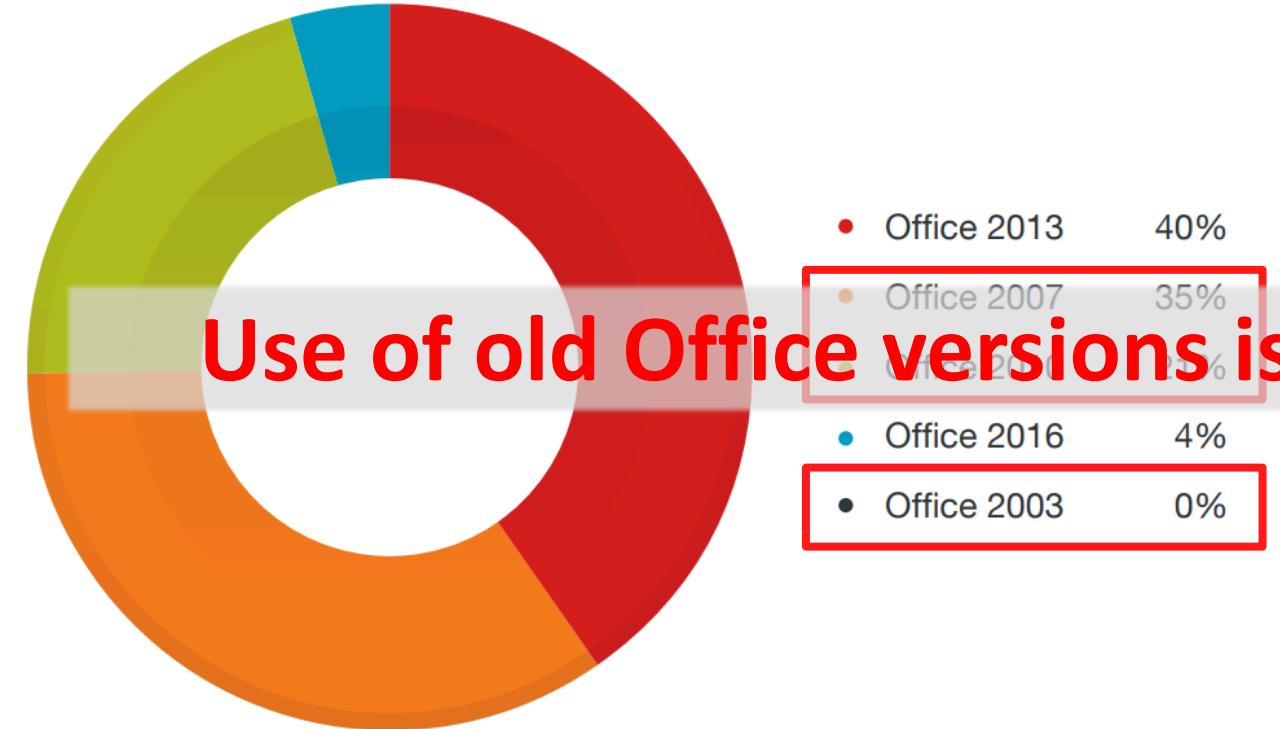
CAD files can be weaponized for espionage

ACM_MEDRE.AA

- Send PST file of Microsoft Outlook to a predefined email address
- Send an opened CAD (DWG) file to a predefined email address

FAS4-FILE ; Do not change it!
967
88 \$9 CW SOU ♥OU SOT ♥S CU

Use of older version of Microsoft Office



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

Version	Support	Default macro behavior	Block from the internet	Trusted locations	Require digital signature	Block per application
Office 2016	Supported until 2025	Block until the user clicks the <i>Enable Macros</i> button	Yes	Yes	Yes	Yes
Office 2013	Supported until 2023	Block until the user clicks the <i>Enable Macros</i> button	Yes*	Yes	Yes	Yes
Office 2010	Supported until 2020	Block until the user clicks the <i>Enable Macros</i> button	Yes	Yes	Yes	Yes
Office 2007	Supported until 2017	Block until the user clicks the <i>Enable Macros</i> button			Yes	Yes
Office 2003	Not supported	Macros run automatically			Yes	Yes

*The feature was added to Office 2013 by Microsoft Update.

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

Distribution of Confidential information

日本企業の文書が掲載されているのは中国の検索サービス大手、百度（バイドゥ）が運営する文書共有サイト「百度文庫」。IT関連会社「クロスワープ」（東京）が調べたところ、2017年6月～18年2月だけで186社の文書掲載が確認された。いずれの資料にも「機密」を意味する注意書きが記されていた。

文書が掲載されていた企業はメーカーからサービス業まで多岐にわたる。製品の設計図や社内研修で使われたとみられる製品機能の説明資料のほか、飲食店チェーンの接客マニュアルもあった。

止ま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/DGXMZO2756453001032018CR8000/>



日本企業の内部文書も掲載されている文書共有サイト
「百度文庫」

インターネットを活用した新しい侵害形態

IP FORWARD

昨今、誰でも自由にワードやエクセル等のデータをアップロードでき、不特定多数の人間がダウンロードできるようになる「文書共有サイト」が急増

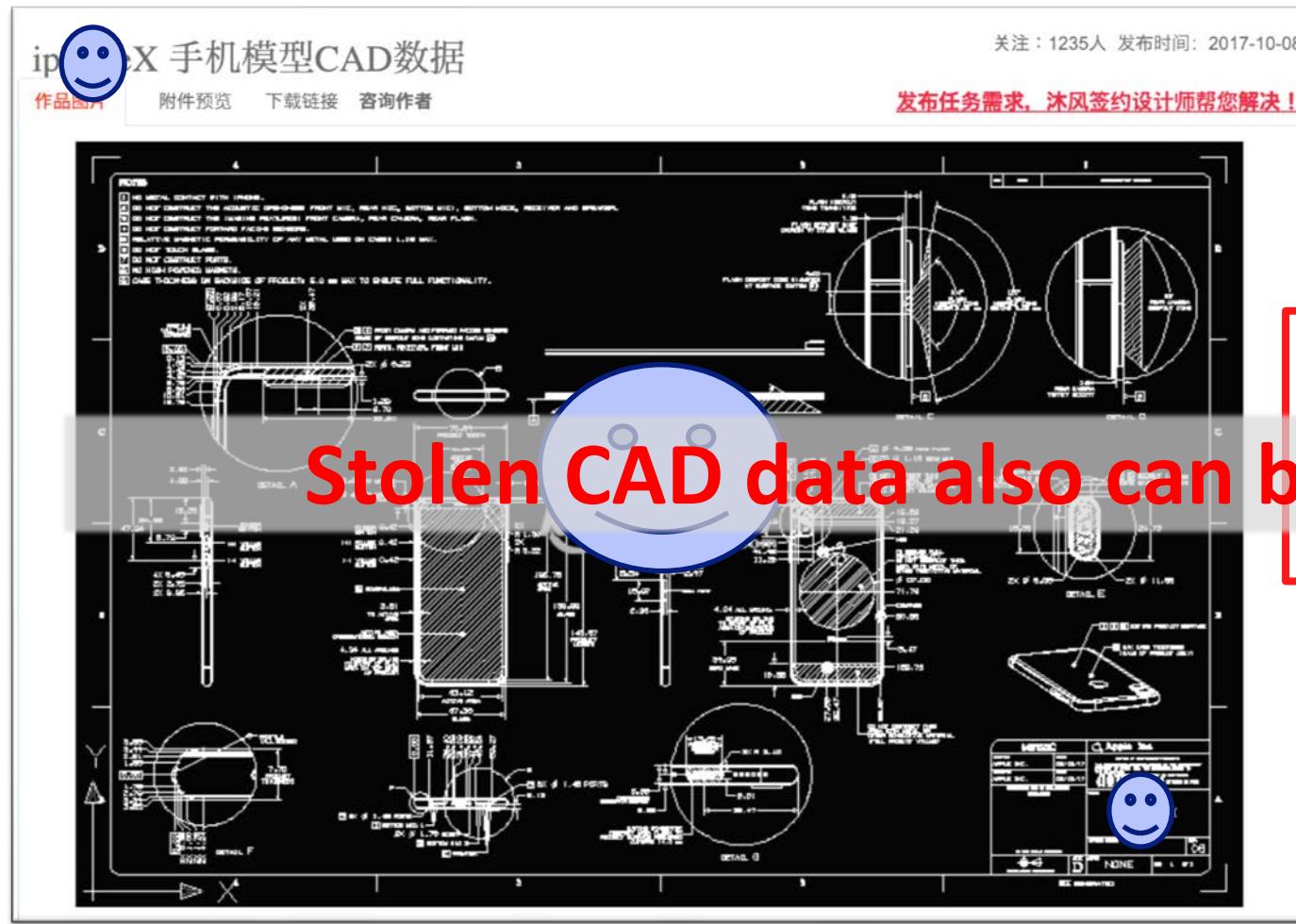
【文書共有サイトの例】



Copyright (C) 2015 IP FORWARD. All Rights Reserved.

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)
<https://www.ipa.go.jp/files/000043950.pdf>

Distribution of leaked CAD files



Sites showing leaked CAD files pertaining to a popular smartphone

Counterfeit products issue

 **UN News**  Global perspective Human stories

Search Advanced Search

HOME TOPICS IN DEPTH SECRETARY-GENERAL MEDIA

Africa Americas Asia Pacific Middle East Europe ICYMI

AUDIO HUB SUBSCRIBE

New UN campaign spotlights links between organized crime and counterfeit goods

COUNTERFEIT

Counterfeit is a serious issue for Manufacturing companies

ORGANIZED CRIME

UNODC 'Counterfeit: Don't buy into organized crime' UNODC campaign.

14 January 2014

The United Nations today launched a new campaign to raise awareness about the links between organized crime and the trade in counterfeit goods, which amounts to \$250 billion a year.

RELATED STORIES

UN crime congress pledges closer cooperation against global threats

\$250billion a year damage worldwide

<https://news.un.org/en/story/2014/01/459622-new-un-campaign-spotlights-links-between-organized-crime-and-counterfeit-goods>

 **INTERPOL**

EN v Q

Illicit goods - the issues

Home > Crimes > Illicit goods > Illicit goods - the issues

Illicit goods - the issues

- Response to illicit
- Illicit goods
- Pharmaceutical operations
- Food crime operations
- Operations against illicit goods
- Training to fight illicit goods
- Illicit goods - Events and partners
- + Shop safely

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.



Profits from the sale of illicit products funds other types of crime

One of major crimes for INTERPOL

<https://www.interpol.int/en/Crimes/Illicit-goods/Illicit-goods-the-issues>

Counterfeit becomes “Supercopy”

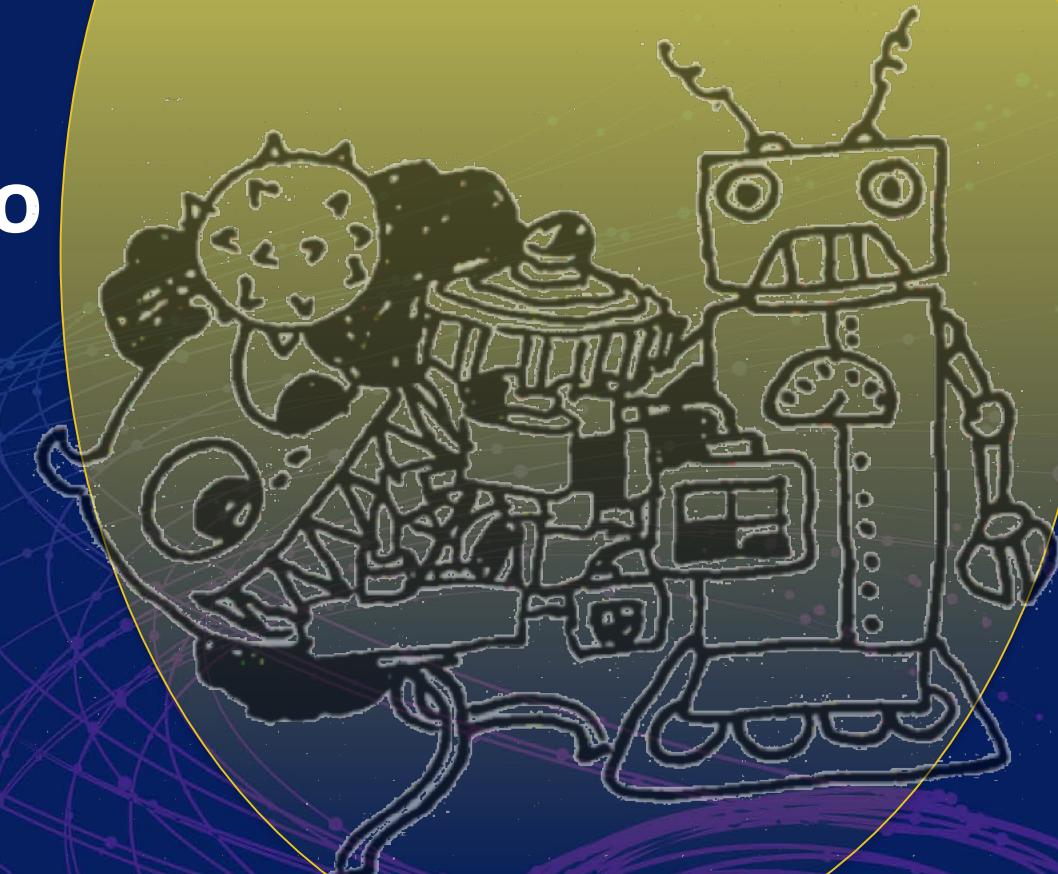


The issue can be more serious in the era of Industry 4.0

潜入！闇のマーケット 中国“スーパーコピー”的衝撃 2016年9月6日
<http://www.nhk.or.jp/gendai/articles/3857/1.html>

RSA® Conference 2019 Asia Pacific & Japan

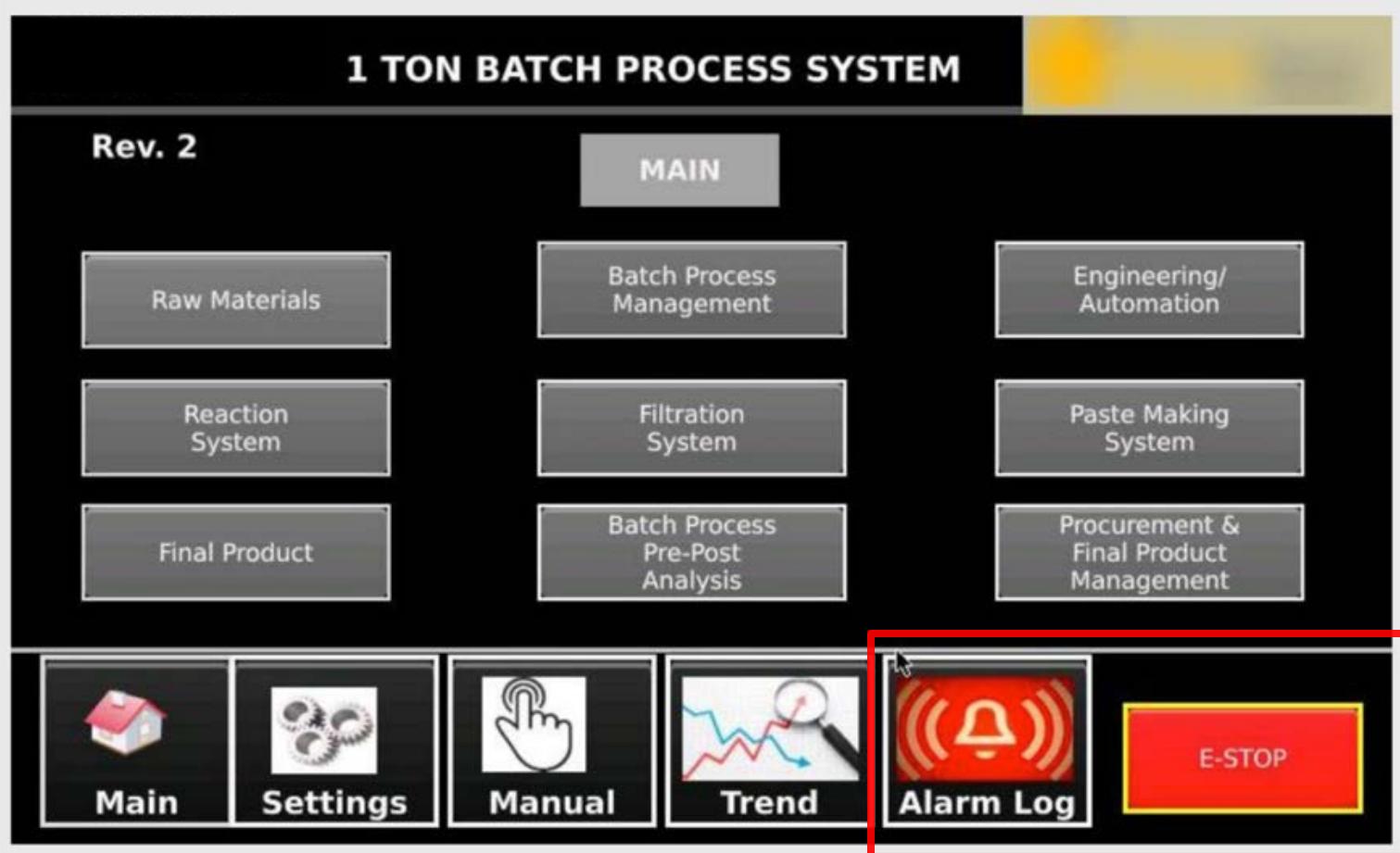
Other Threats and Risks to exposed OT systems







Exposed ICSs



RSA® Conference 2019 Asia Pacific & Japan

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 .

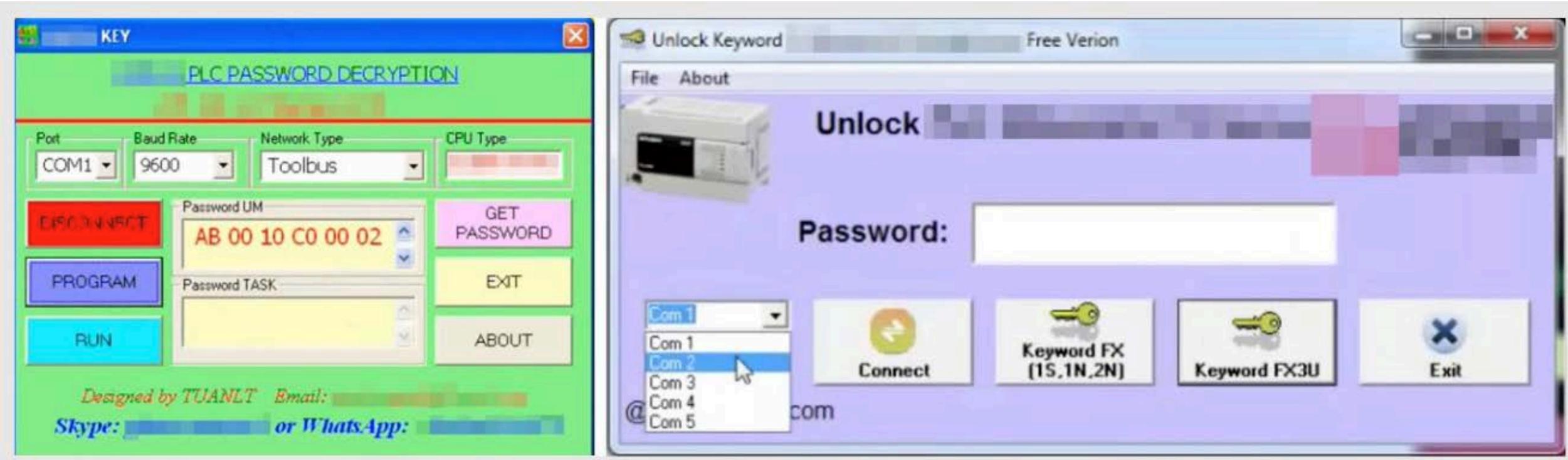


4t4k4

Newbie

Good day to all. interested in o-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. Im 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.

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.029 ₩	<input type="button" value="1 X"/> Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.059 ₩	<input type="button" value="1 X"/> Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites	900 EUR = 0.106 ₩	<input type="button" value="1 X"/> Buy now
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.	200 EUR = 0.024 ₩	<input type="button" value="1 X"/> Buy now

Industrial equipment purchase request

10.05.2018, 21:22 # 1

CobaltDron
Newbie



[Buy] Need to drive the equipment

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 3-15т.р.
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

Group: Members
Joined: 15-February-2013
0 posts
Thanks: 9
Thanked 2 Times in 2 Posts
Put by (2) Dislajk: 2
Пославили Дизлайк 0 times in 0 posts
Reputation: 1

Shodan Shop with Industrial Section

ⓘ Not Secure | shodanshop.com/primery-poiska-v-shodan-analiz-schneider-electric/

the main Contacts Score Webcams Industry Modems Printers
Servers

With Google search, we determine that we are invited to log in by the **industrial VPN router**
eWON, with the login **account adm** and the password **adm**.

ewON

Information	
User	(Adm)
LAN IP/Mask	192.168.1.18/255.255.255.0
Serial Number	1550-0003-52
Current time	19/11/2016 14:18:27
Firmware Version	EW_8_2a1

Transparent Forwarding	
Connect To:	0.0.0.0
<input type="button" value="Connect"/> <input type="button" value="Clear transp. forwarding"/>	

Internet: Modem Connection	
Internet Connection:	Ip Address: [REDACTED] Connected since: 0:00:27:17
<input type="button" value="Close Internet Connection"/>	

teamkelvinsecteam

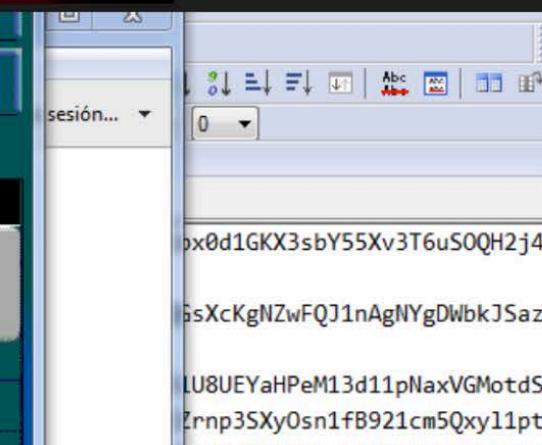
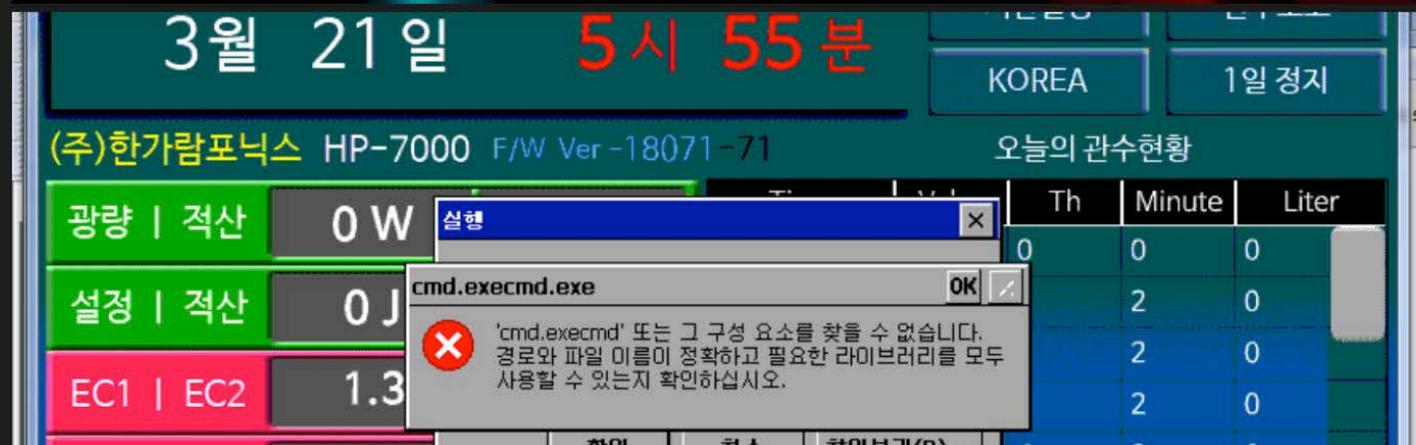


KelvinSecTeam Hackers

Posts	712
Threads	632
Joined	Apr 2018
Reputation	143

1 YEAR OF SERVICE

★ 03-20-2019, 10:05 PM

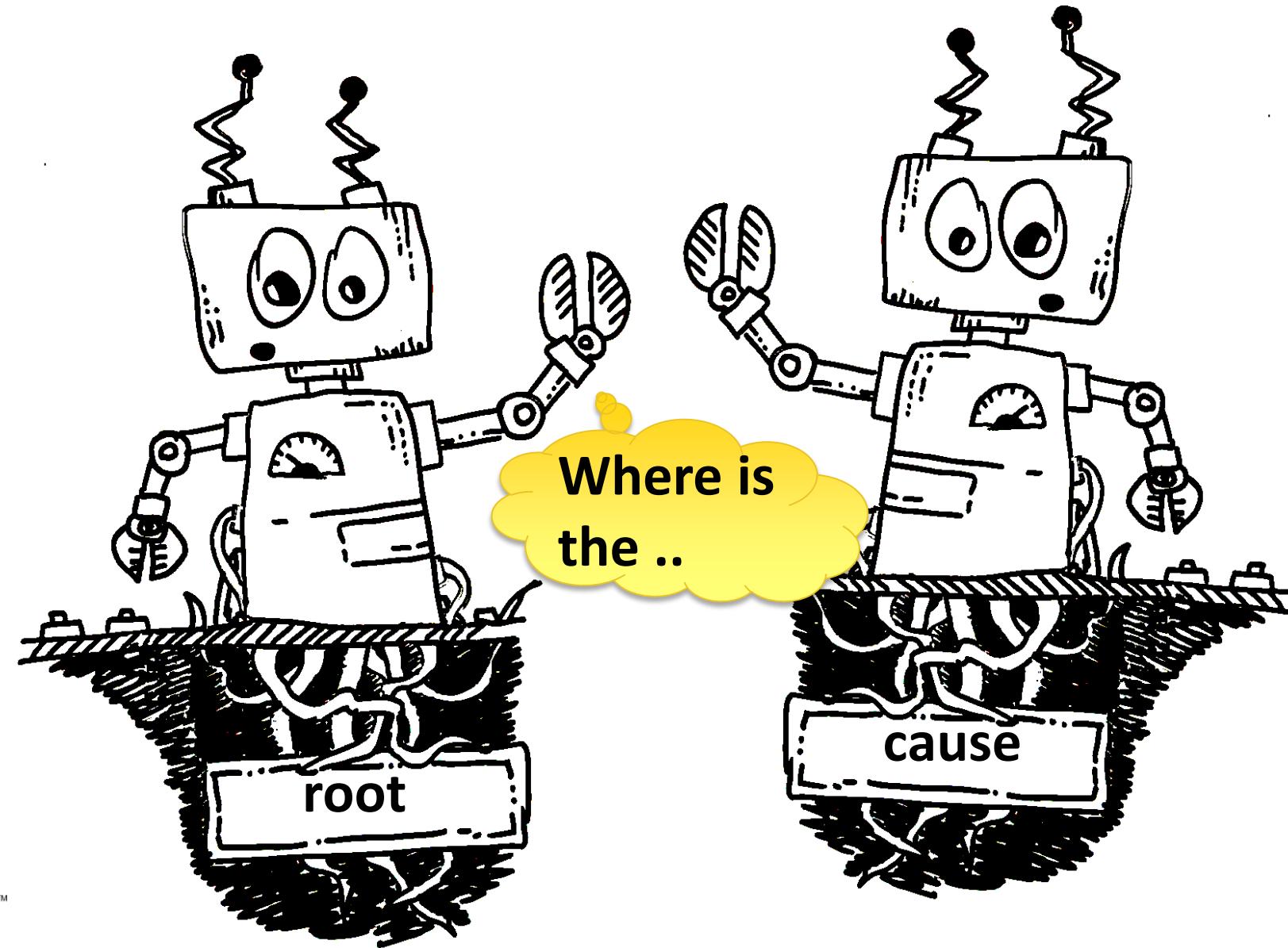


RSA® Conference 2019 **Asia Pacific & Japan**

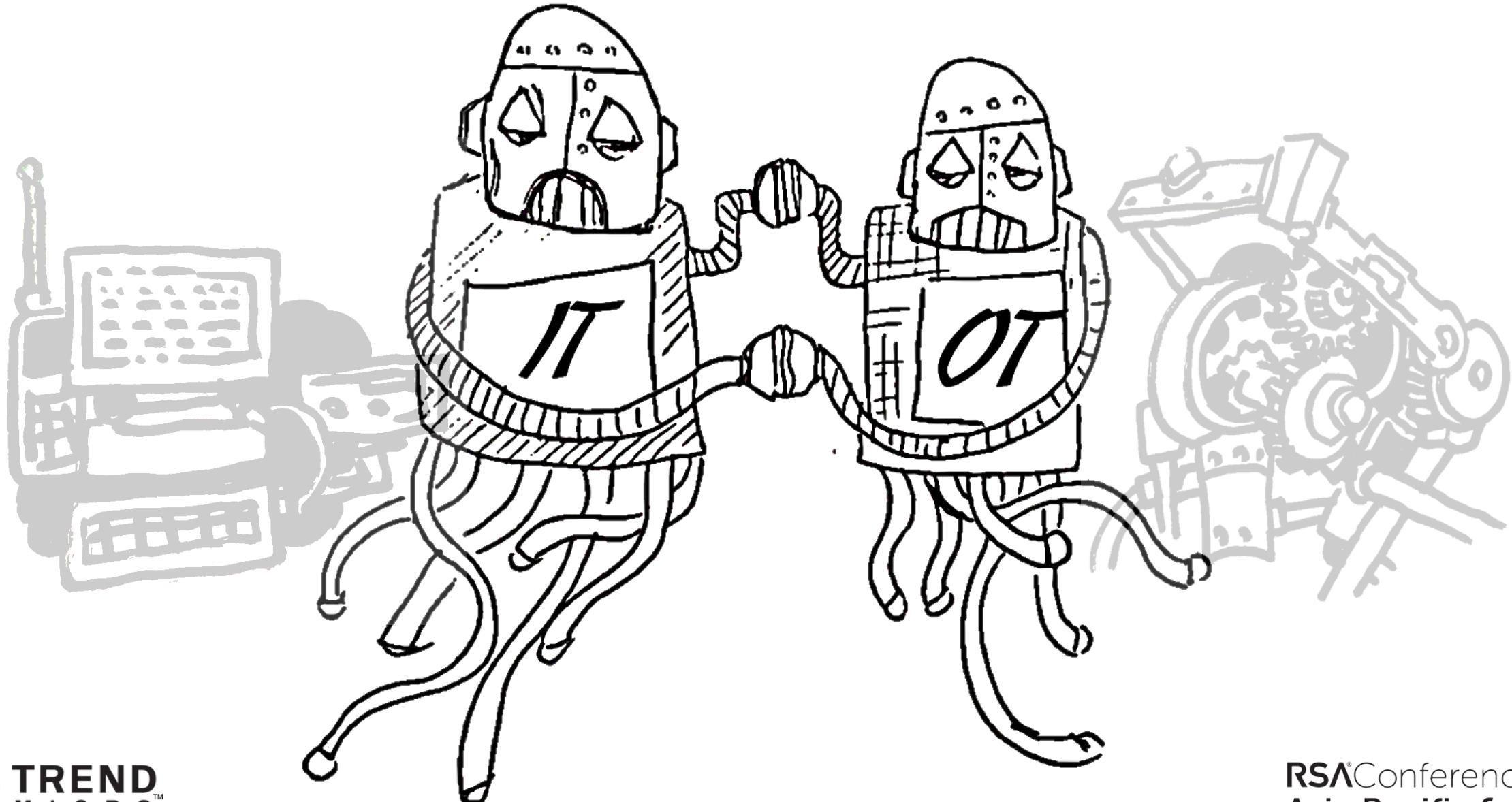
**Examining the root causes and best
practices**

And answer the question “WHY”

THE ROOT CAUSE



Interconnection between IT and OT

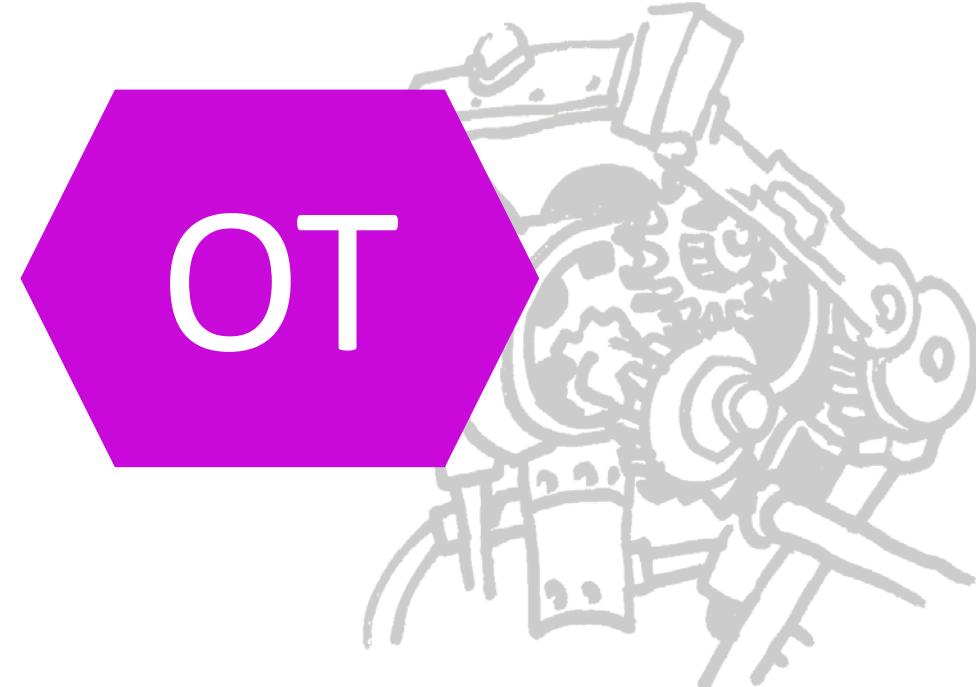
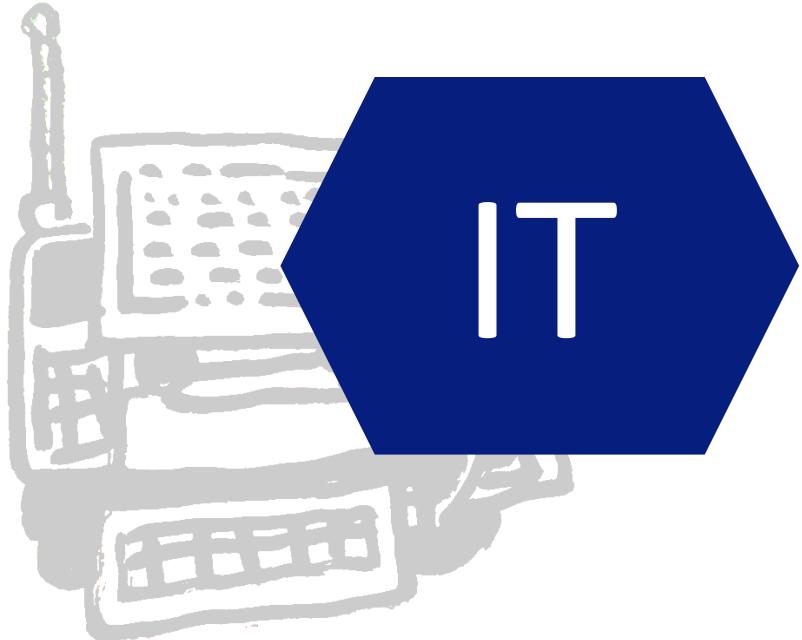


Equipment Lifecycle

3-5 years

VS

26-34 years



Stay UP TO DATE

Windows XP is 17 years old

757,000

Windows XP

Windows Vista
Windows 2000

Threat Modeling: identify Information flows

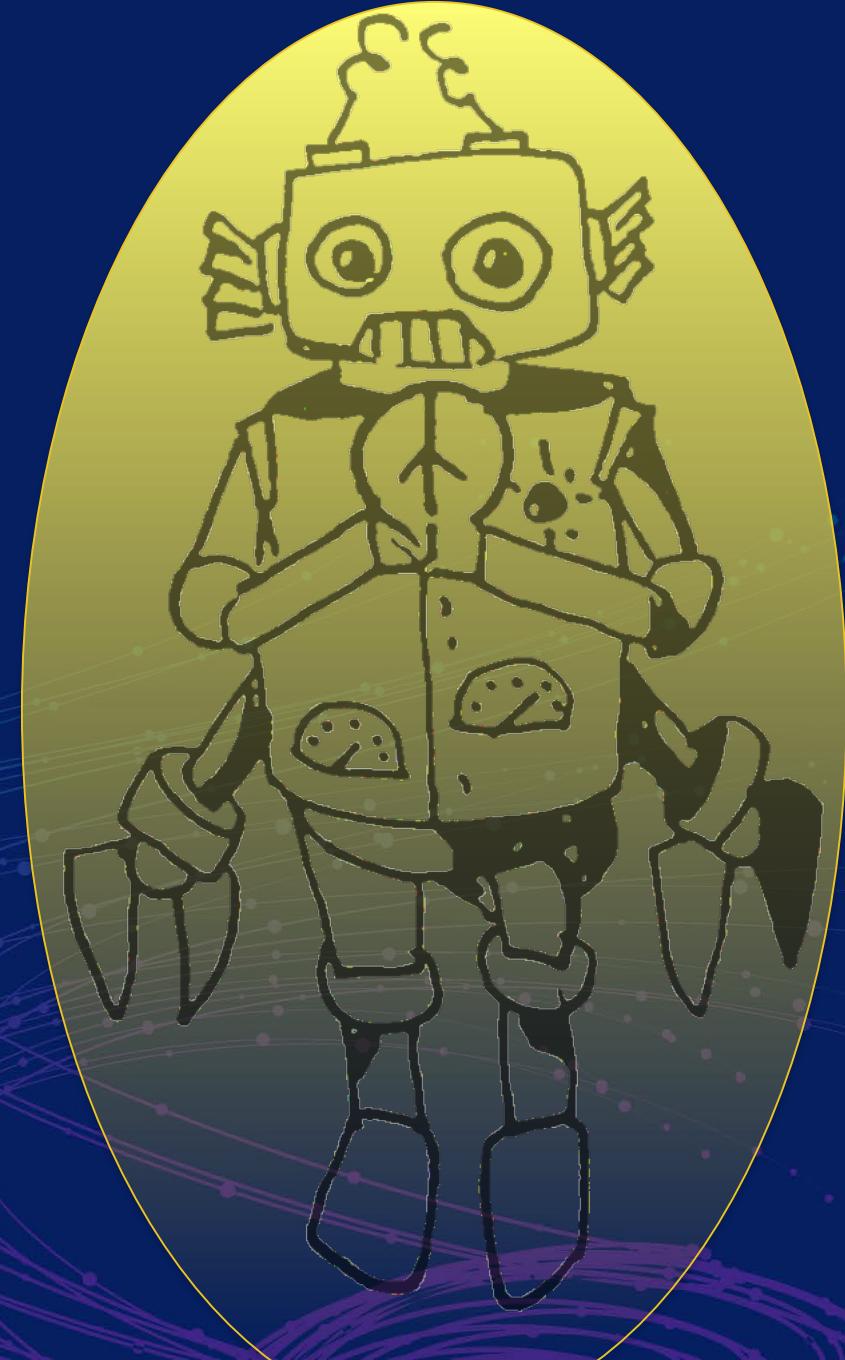
- Think like a hacker: How could Intellectual Property Information be exfiltrated from my network?
- What are the information flow channels?
- What are controls that allow me to prevent this?

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

RSA® Conference 2019 Asia Pacific & Japan

Security Recommendations For Manufacturing



Basic Security Principles

Restrict user access and permissions

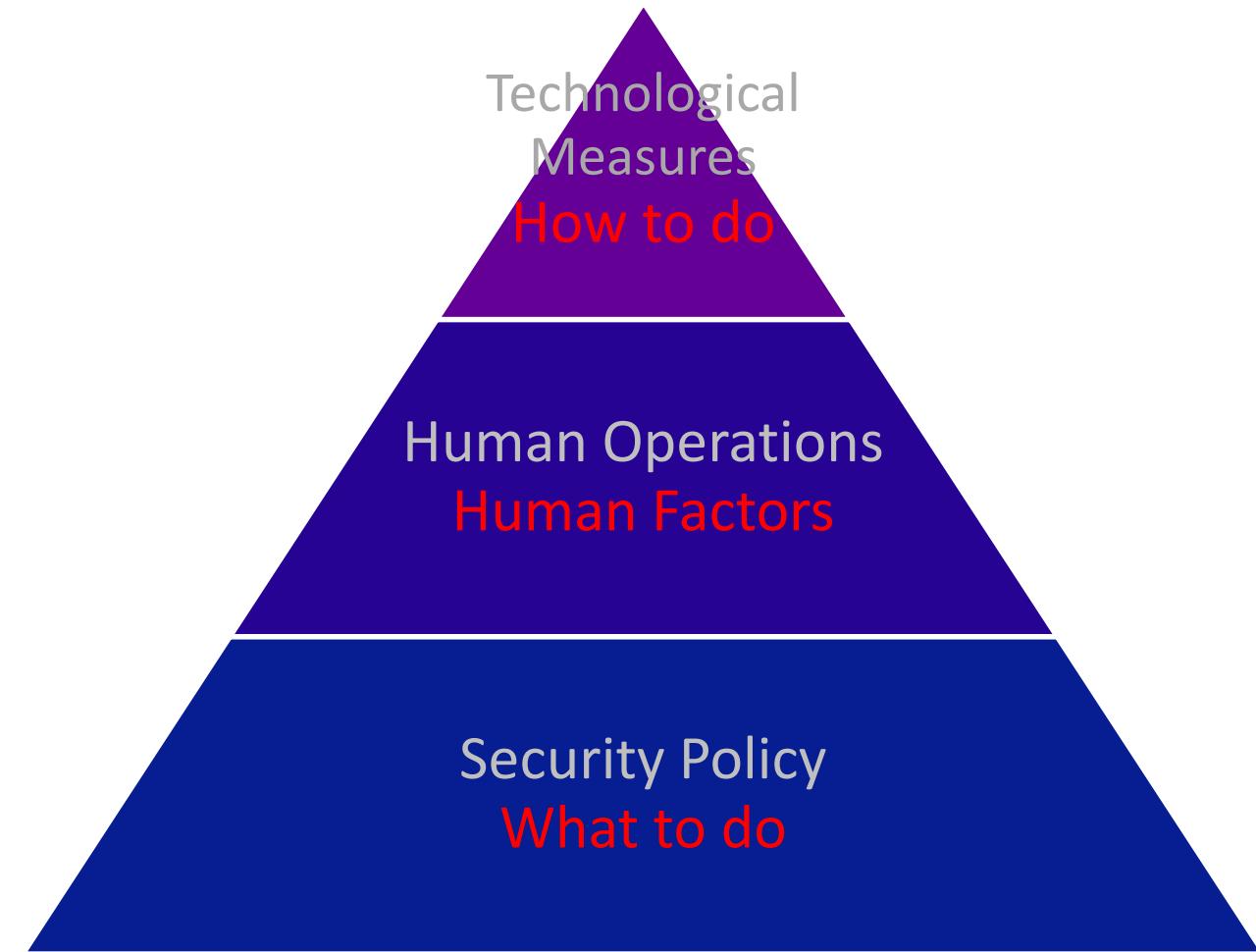
Enforce domain or subnetwork restrictions

Basic Security
Principles

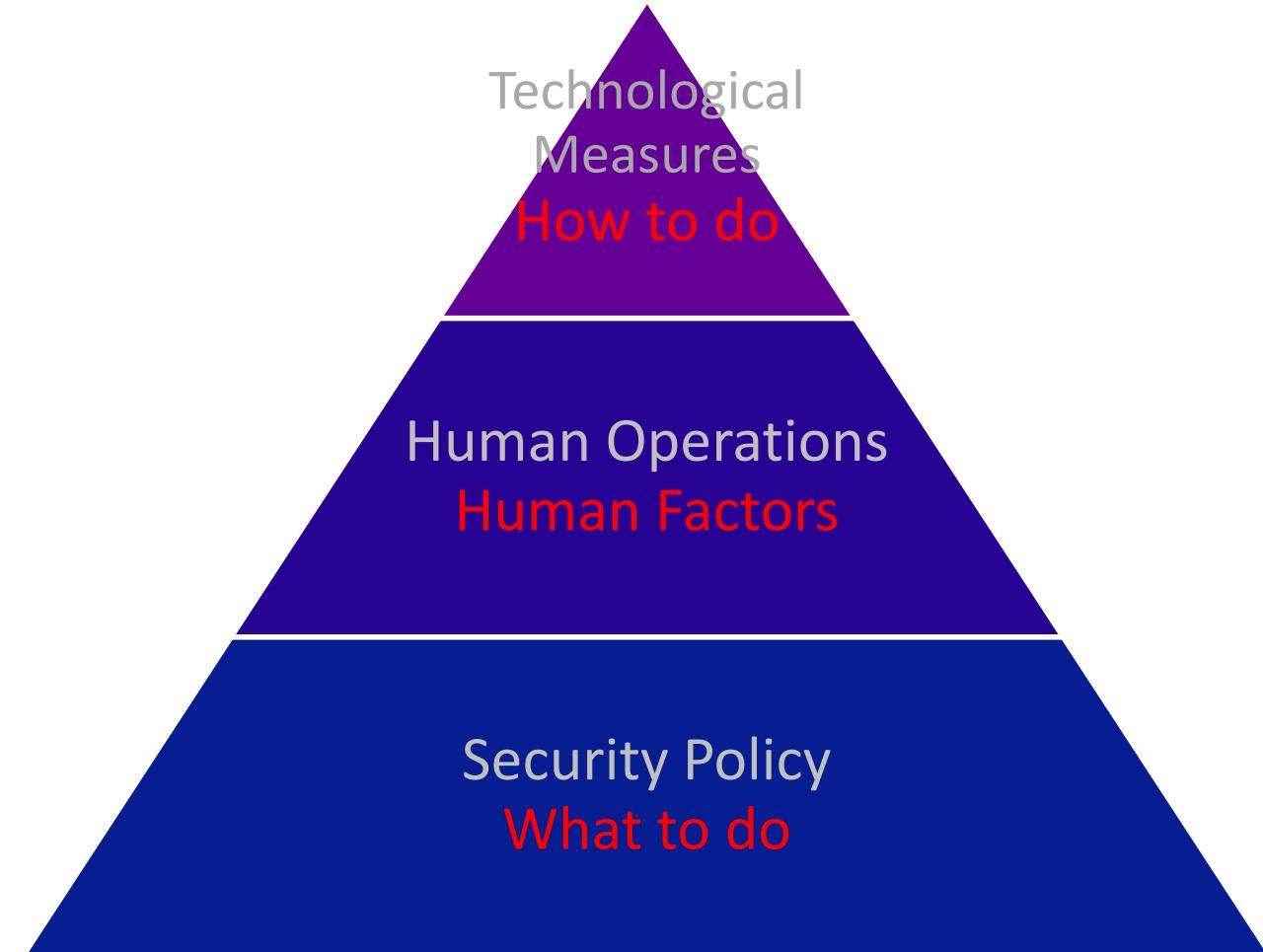
Disable directory listing

Remove or disable unnecessary services

Security Recommendations for Manufacturing

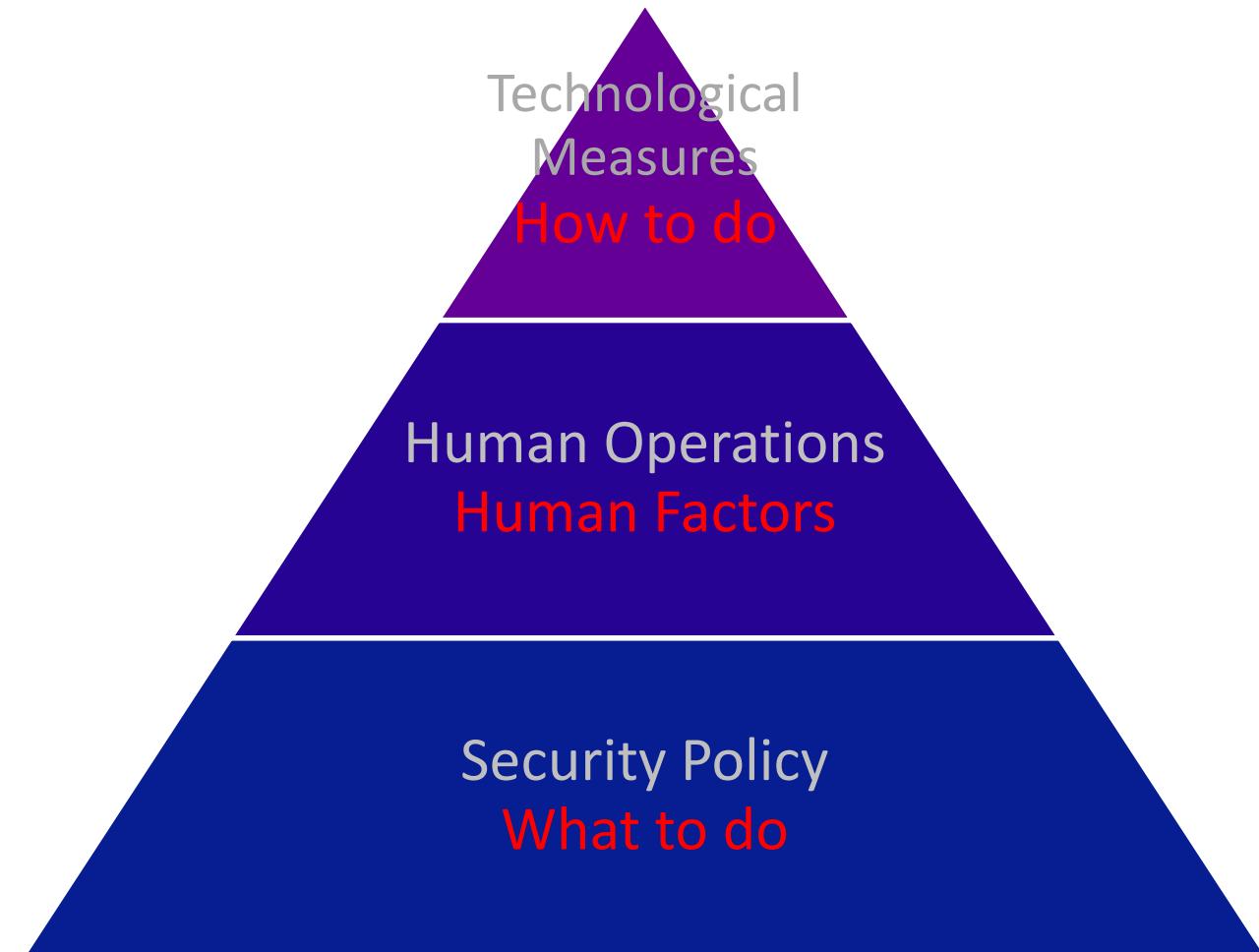


Security Recommendations for Manufacturing



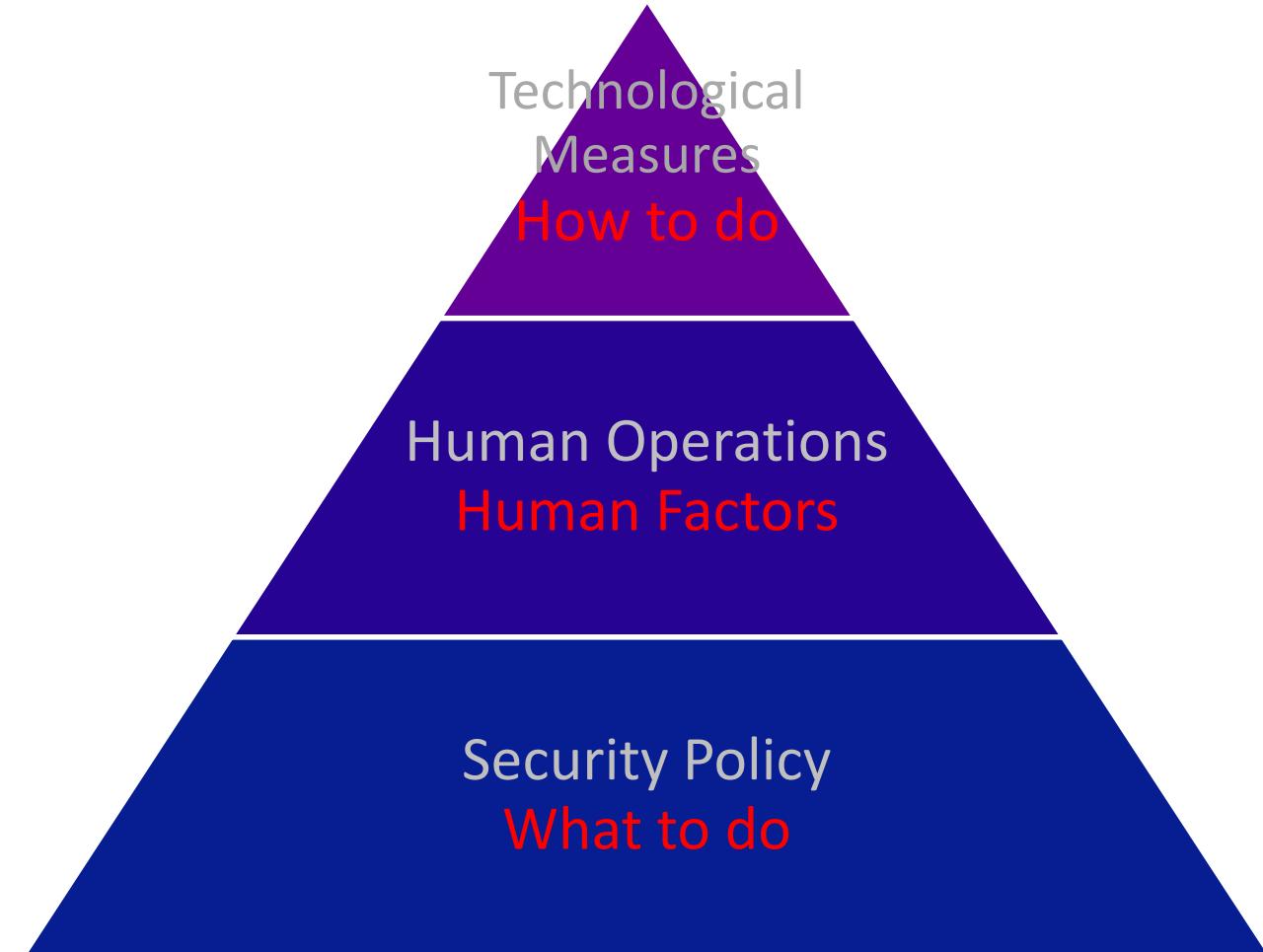
- Accounting and Prioritization of Assets
- Making Security a Requirement
- IEC 62443 Compliance

Security Recommendations for Manufacturing



- User Education
 - Cooperation between IT and OT
-
- Accounting and Prioritization of Assets
 - Making Security a Requirement
 - IEC 62443 Compliance

Security Recommendations for Manufacturing



- Application of Appropriate Protection
- User Education
- Cooperation between IT and OT
- Accounting and Prioritization of Assets
- Making Security a Requirement
- IEC 62443 Compliance

RSA® Conference 2019 Asia Pacific & Japan

Conclusions and Final Remarks

Myth Buster

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

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