31ST ANNUAL FIRST CONFERENCE

EDINBURGH
JUNE 16-21
2019

Attacks on Industrial and Manufacturing Networks

Bakuei Matsukawa, Vladimir Kropotov, Fyodor Yarochkin and Ryan Flores

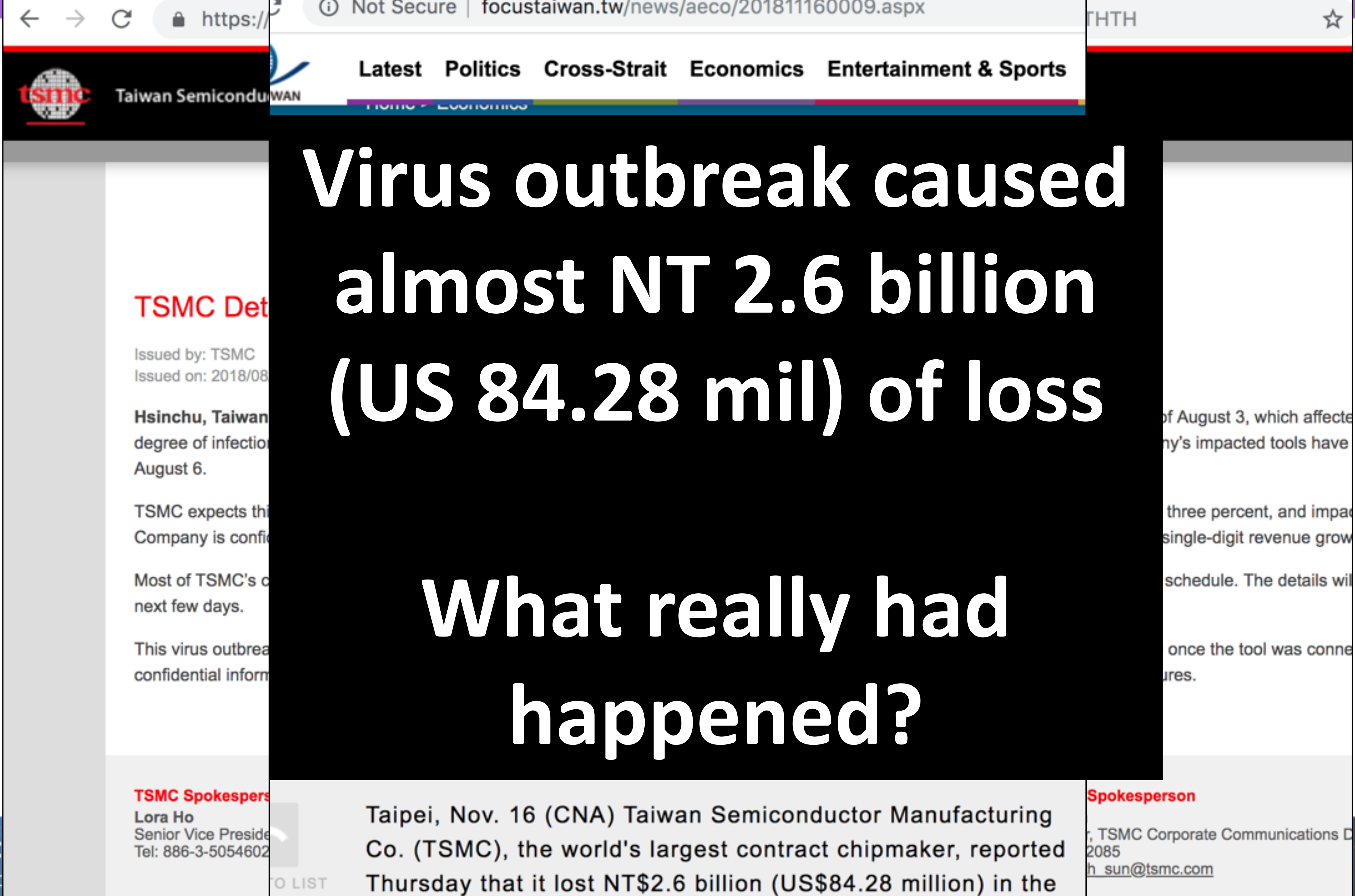
Trend Micro Research

An incident in Taiwan in 2018

Quick introduction for risks of Manufacturing industry

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

What really had happened?



TSMC Det

Issued by: TSMC
Issued on: 2018/08

Hsinchu, Taiwan … of August 3, which affecte
degree of infectio… ny's impacted tools have
August 6.

TSMC expects thi… three percent, and impa
Company is confi… single-digit revenue grow

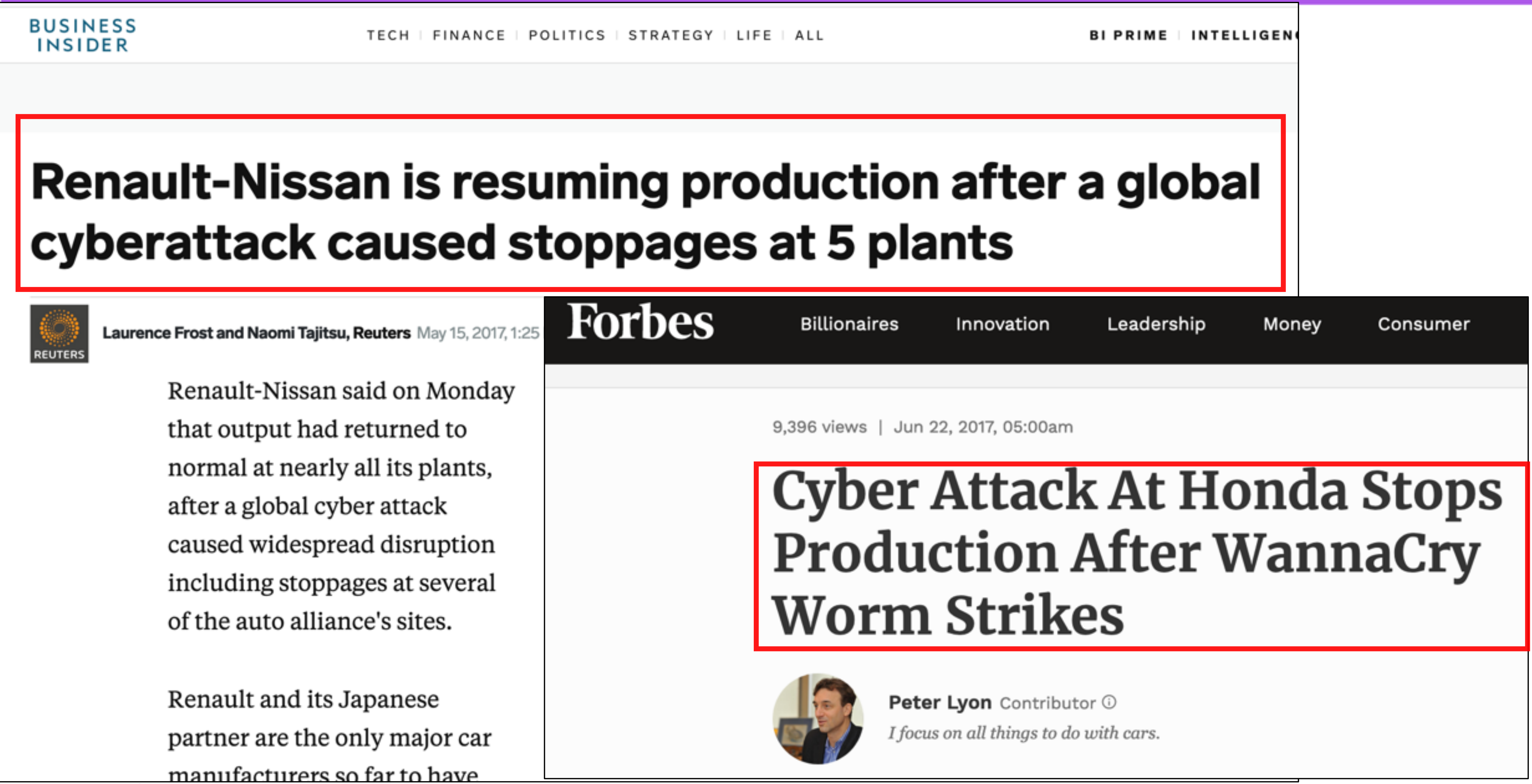
Most of TSMC's … schedule. The details wi
next few days.

This virus outbrea… once the tool was conne
confidential inform… ures.

TSMC Spokespers
Lora Ho
Senior Vice Preside
Tel: 886-3-5054602

Spokesperson
, TSMC Corporate Communications D
2085
h_sun@tsmc.com

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



BUSINESS INSIDER

TECH | FINANCE | POLITICS | STRATEGY | LIFE | ALL

BI PRIME | INTELLIGENC

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

REUTERS

Laurence Frost and Naomi Tajitsu, Reuters May 15, 2017, 1:25

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

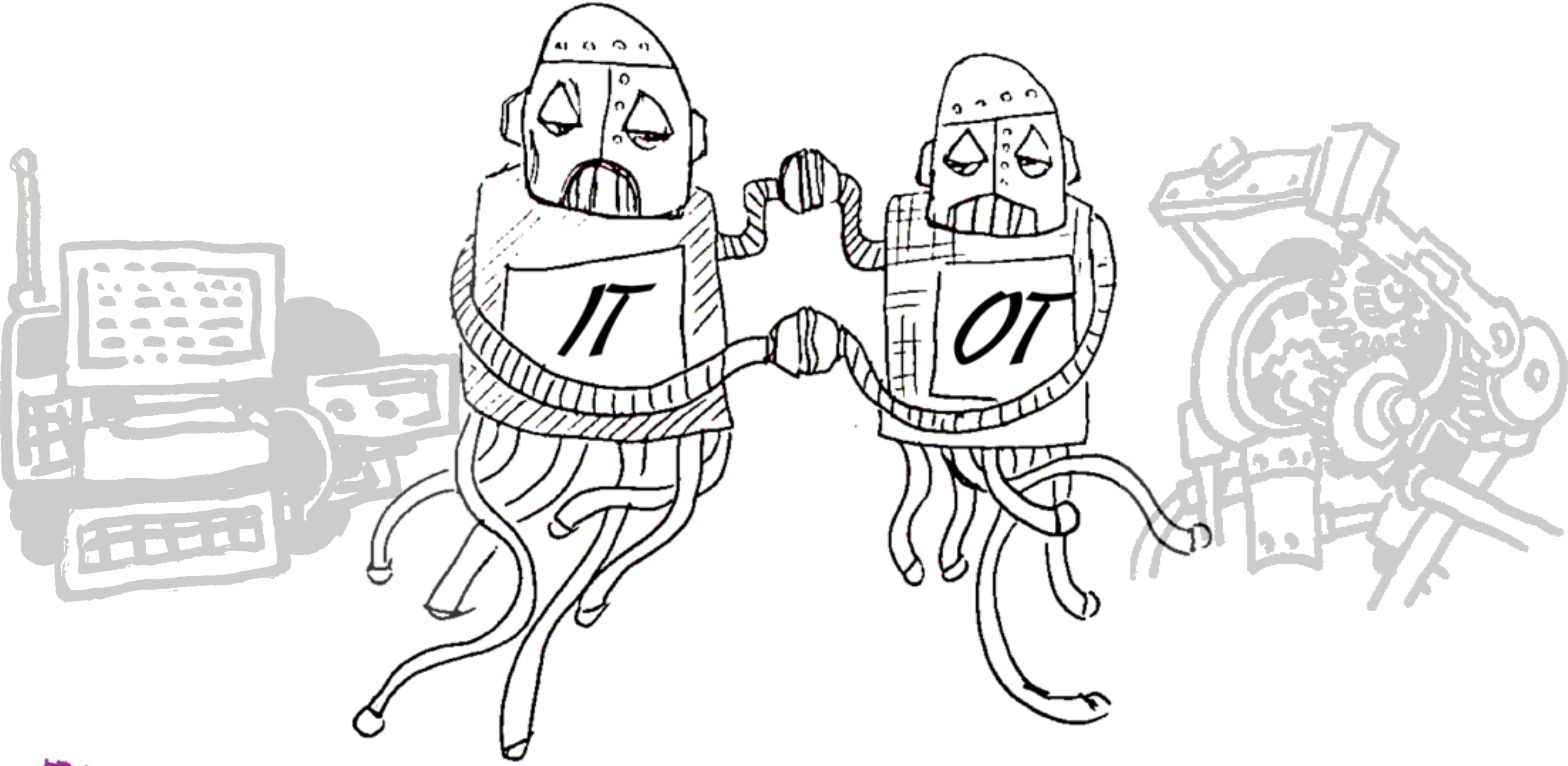
Cyber Attack At Honda Stops Production After WannaCry Worm Strikes

Peter Lyon Contributor ⓘ

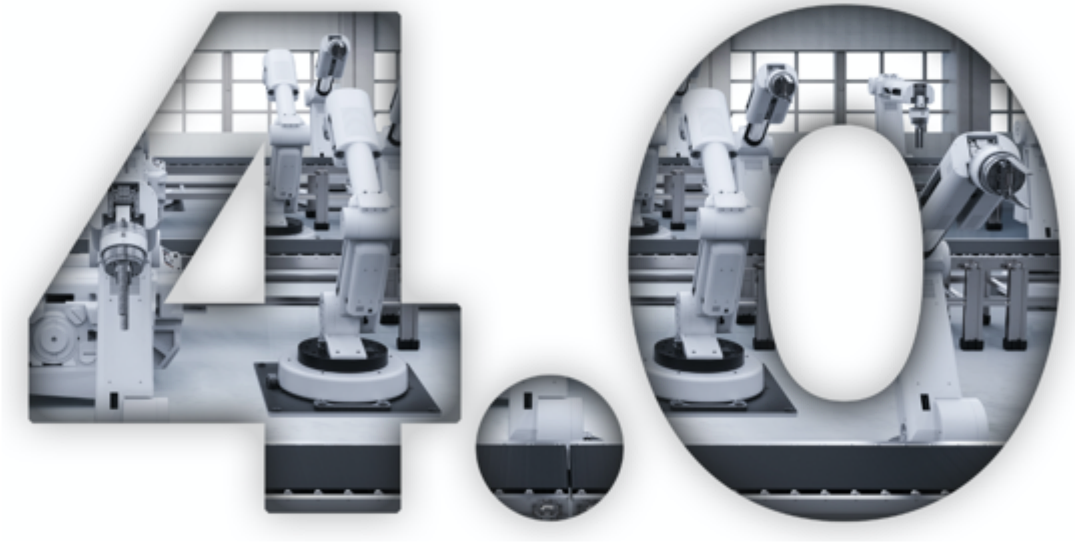
I focus on all things to do with cars.

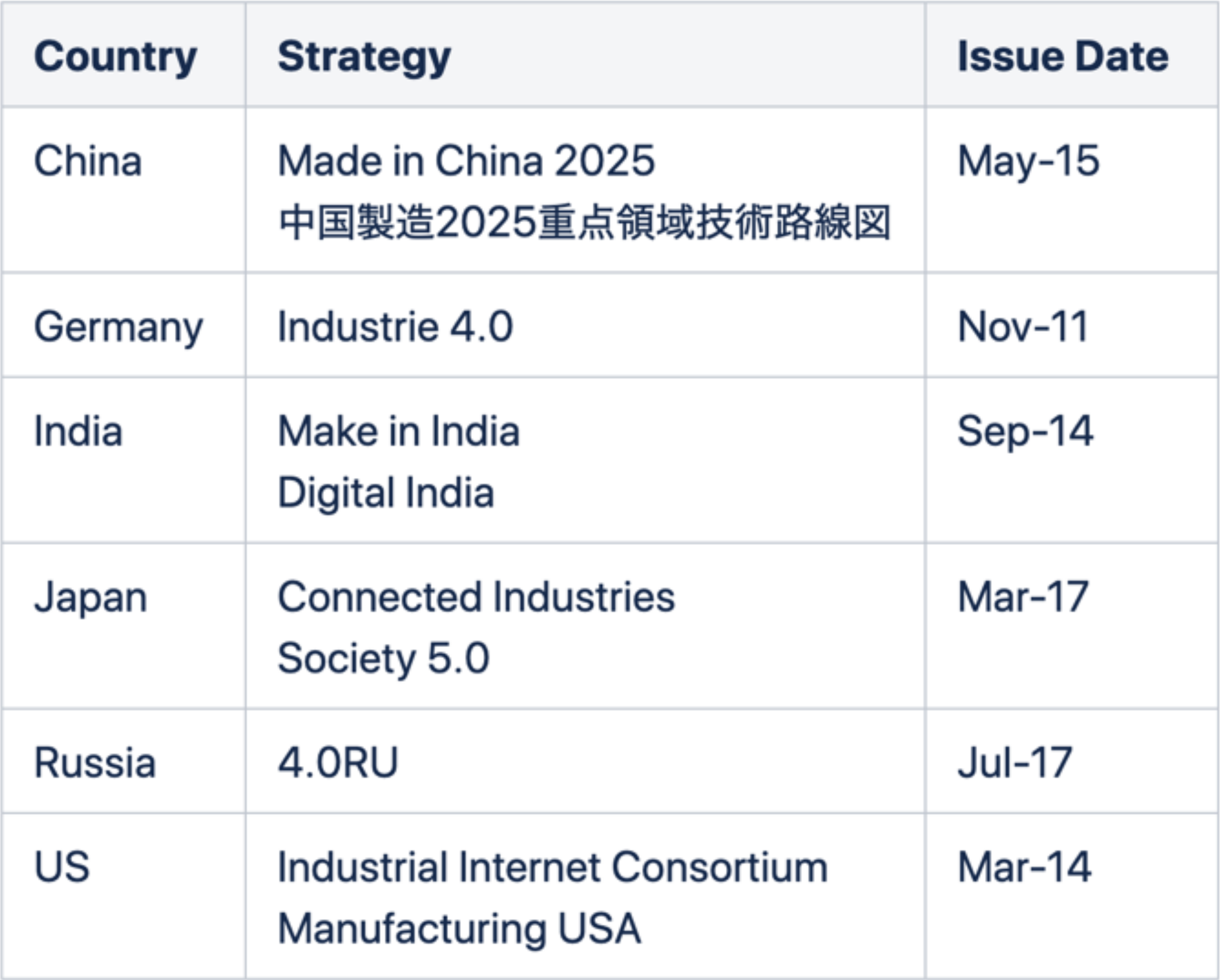
What are the factors that made it happen?

Interconnection between IT and OT



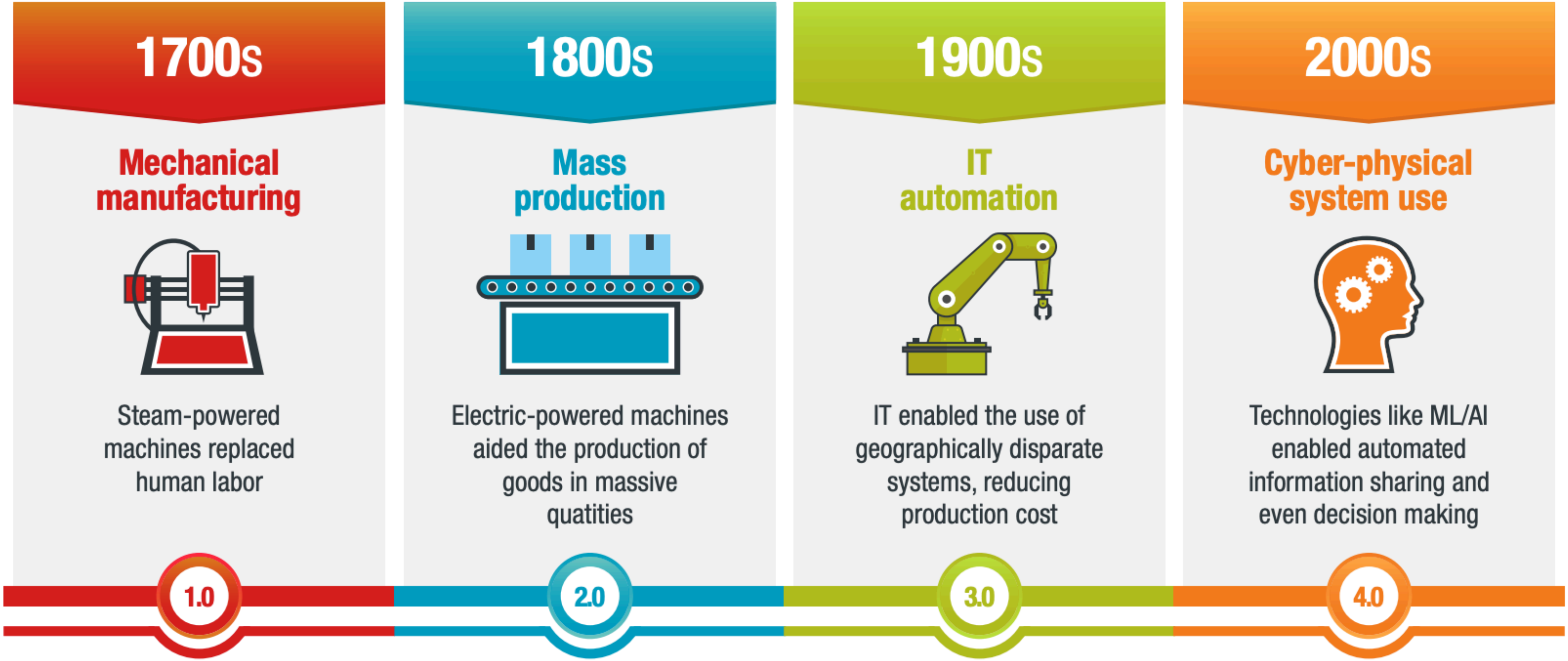
Is Industry 4.0 a Buzzword? – No





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

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 quatities

2.0

1900s

IT automation

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

3.0

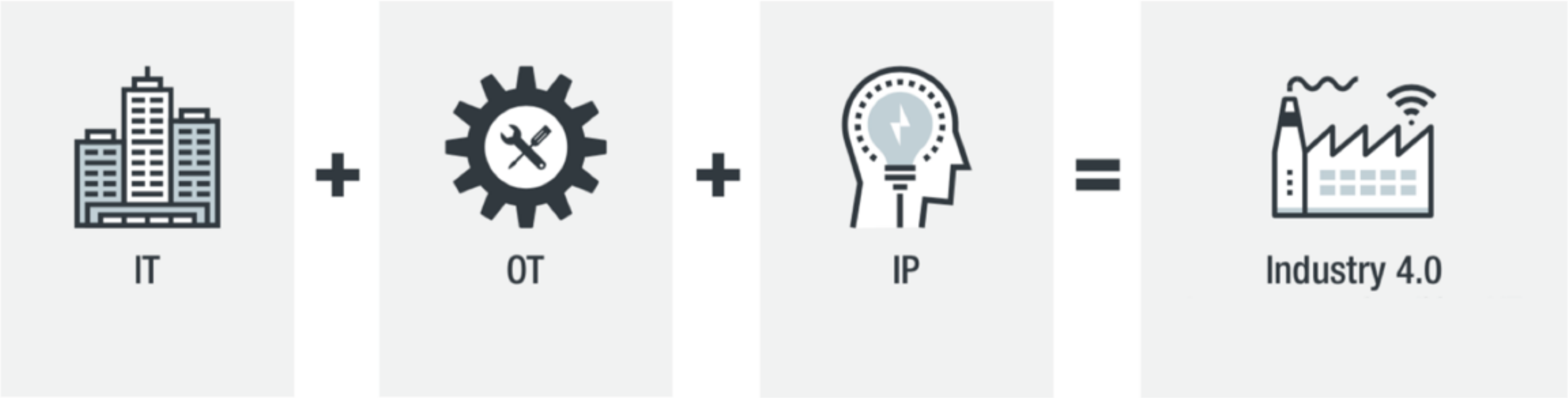
2000s

Cyber-physical system use

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

4.0

Convergence of IT, OT and IP



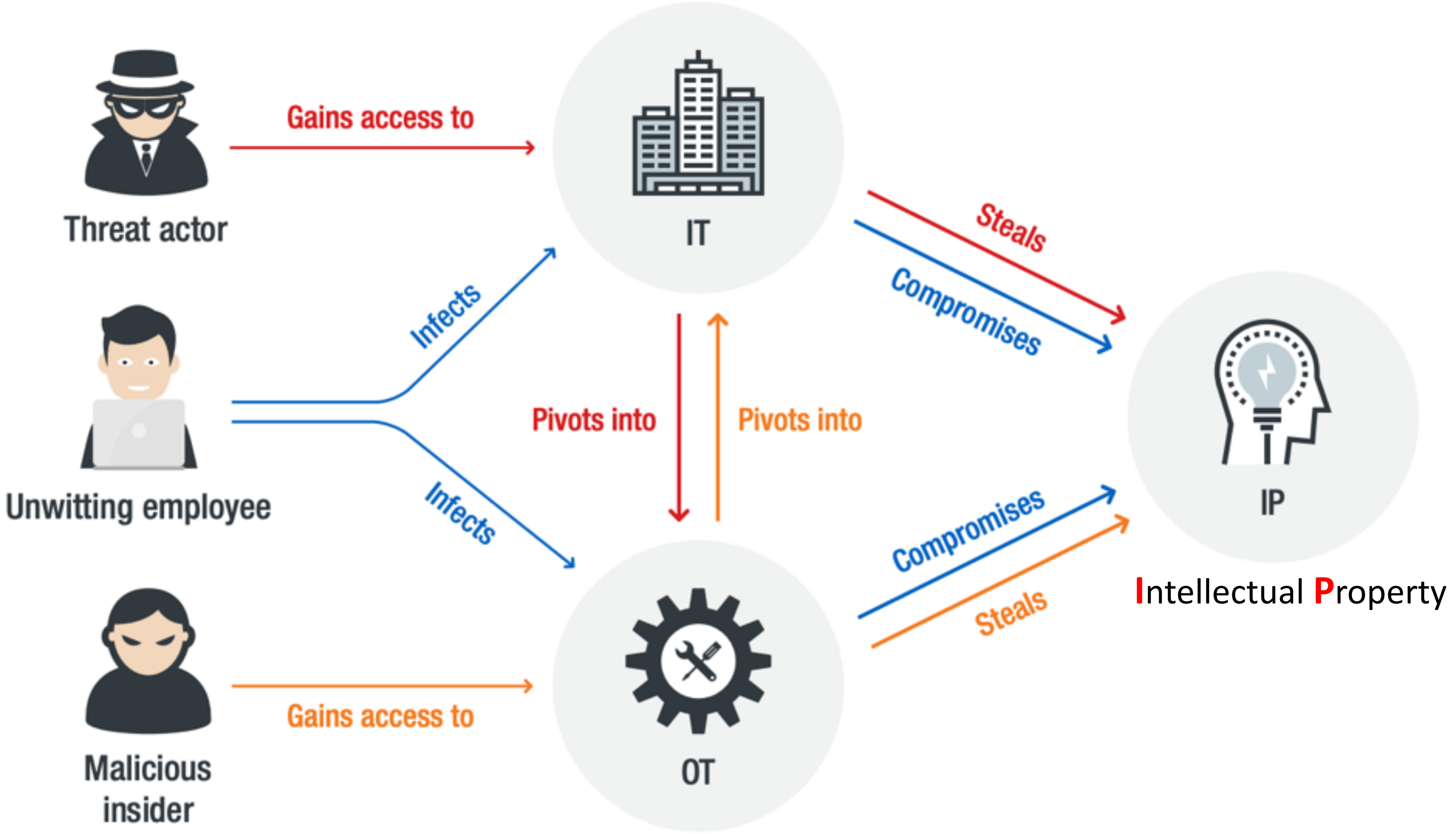
Information **T**echnology

Operational **T**echnology

Intellectual **P**roperty

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

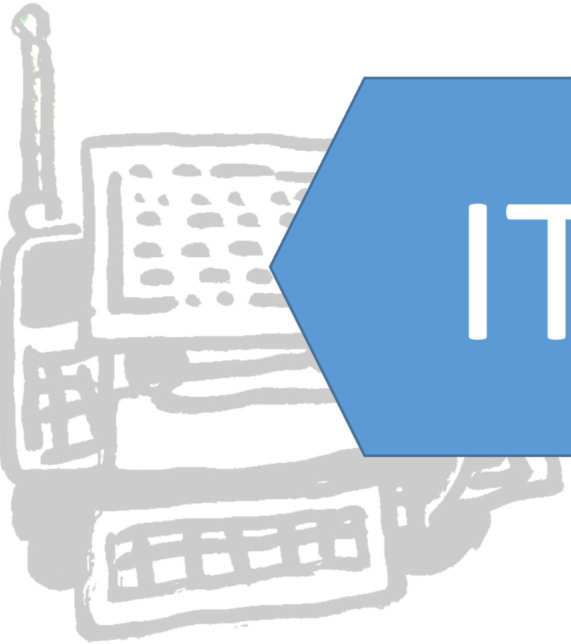
How threats can figure into the convergence



Characteristics of Manufacturing Industry

Unique threat landscape to Manufacturing Industry

Equipment Lifecycle



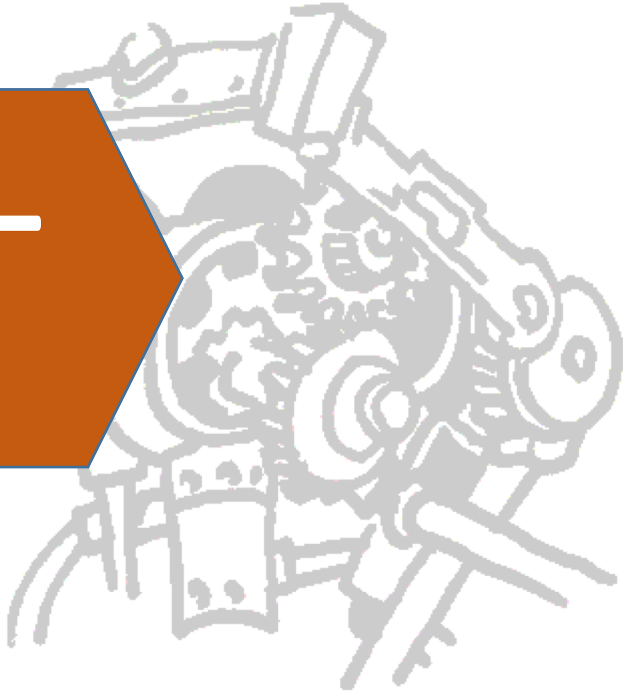
3-5 years

IT

vs

26-34 years

OT



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

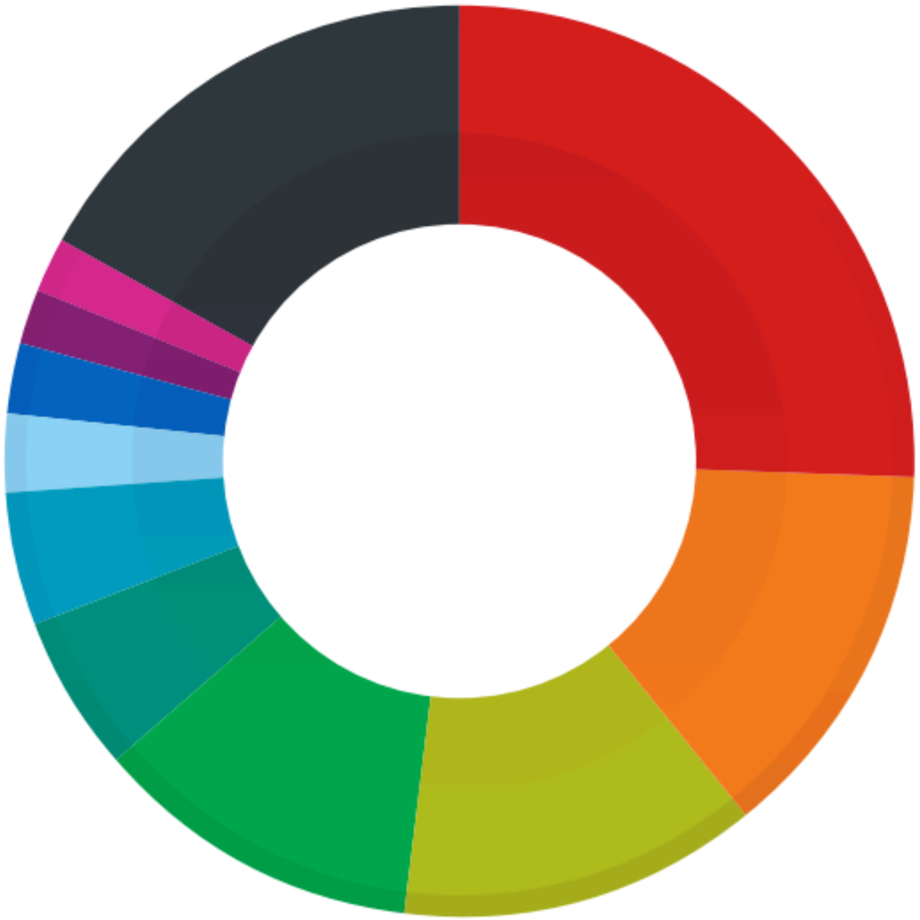
Prevalence of Downad in Manufacturing

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

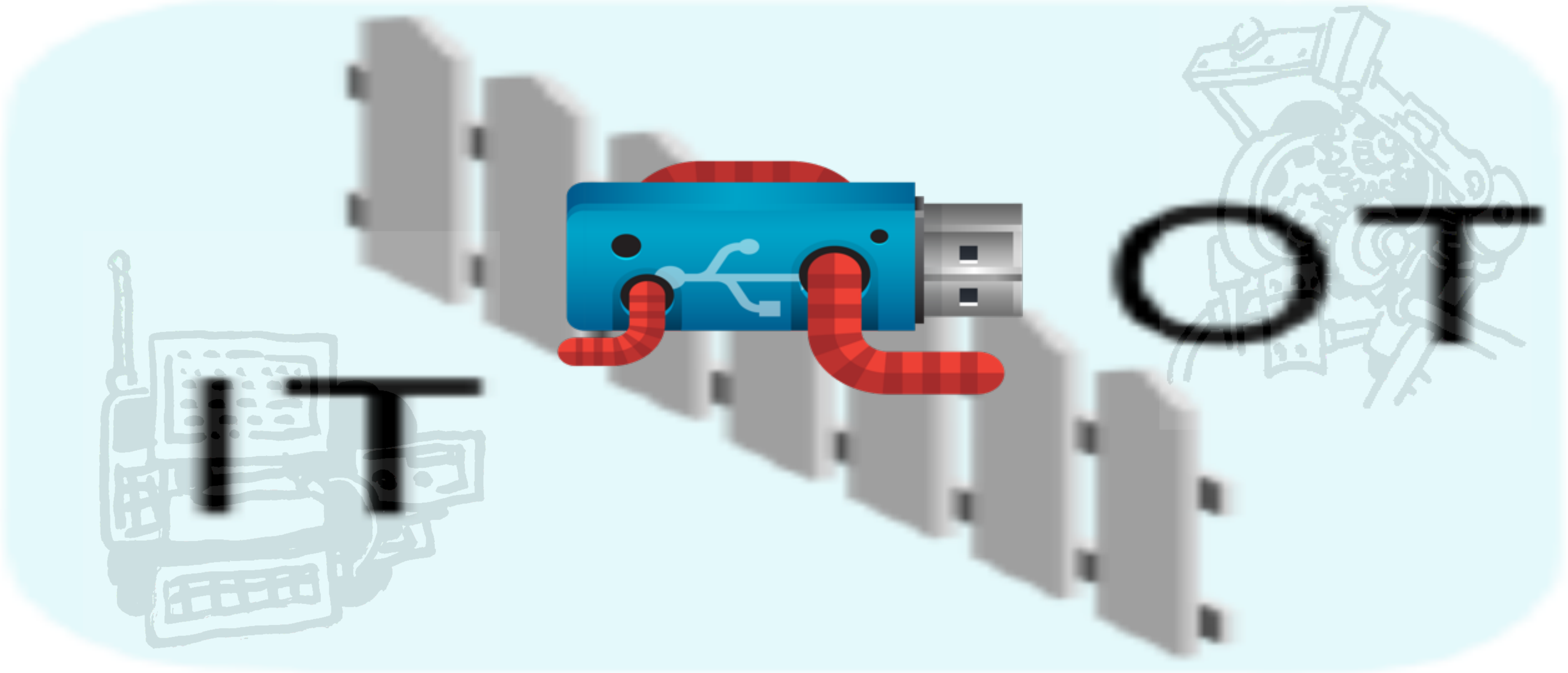
Malicious Autorun.inf detections



●	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

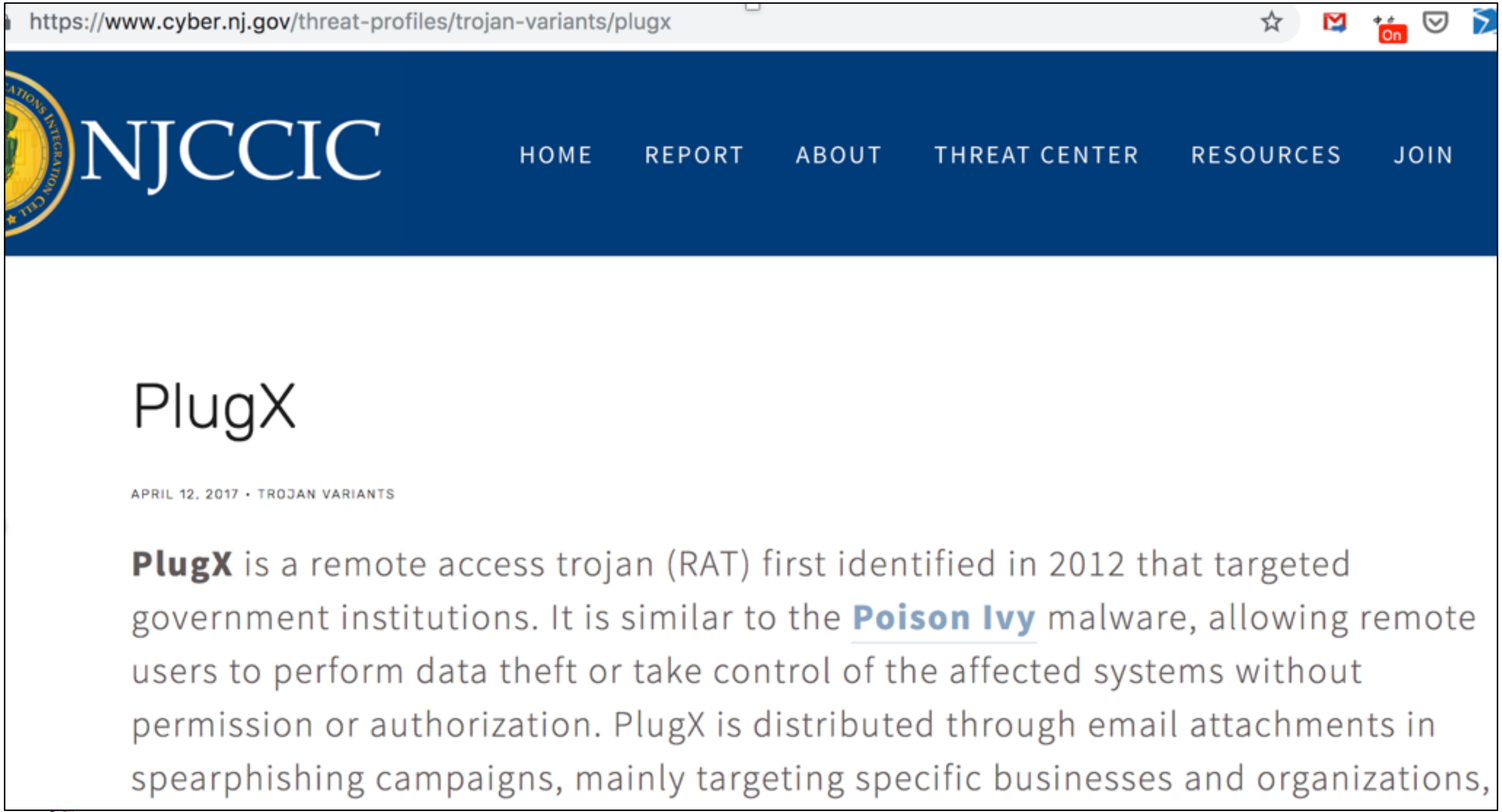
Data exchange via USB between IT and OT



Case study for Manufacturing Industry

PlugX for Ransomware

PlugX on Manufacturing Network



https://www.cyber.nj.gov/threat-profiles/trojan-variants/plugx
NJCCIC
HOME
REPORT
ABOUT
THREAT CENTER
RESOURCES
JOIN

PlugX

APRIL 12, 2017 • TROJAN VARIANTS

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" we 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
- Victim: a manufacturing enterprise in **China**

PlugX for 9.5 Bitcoins ransom

- A similar 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

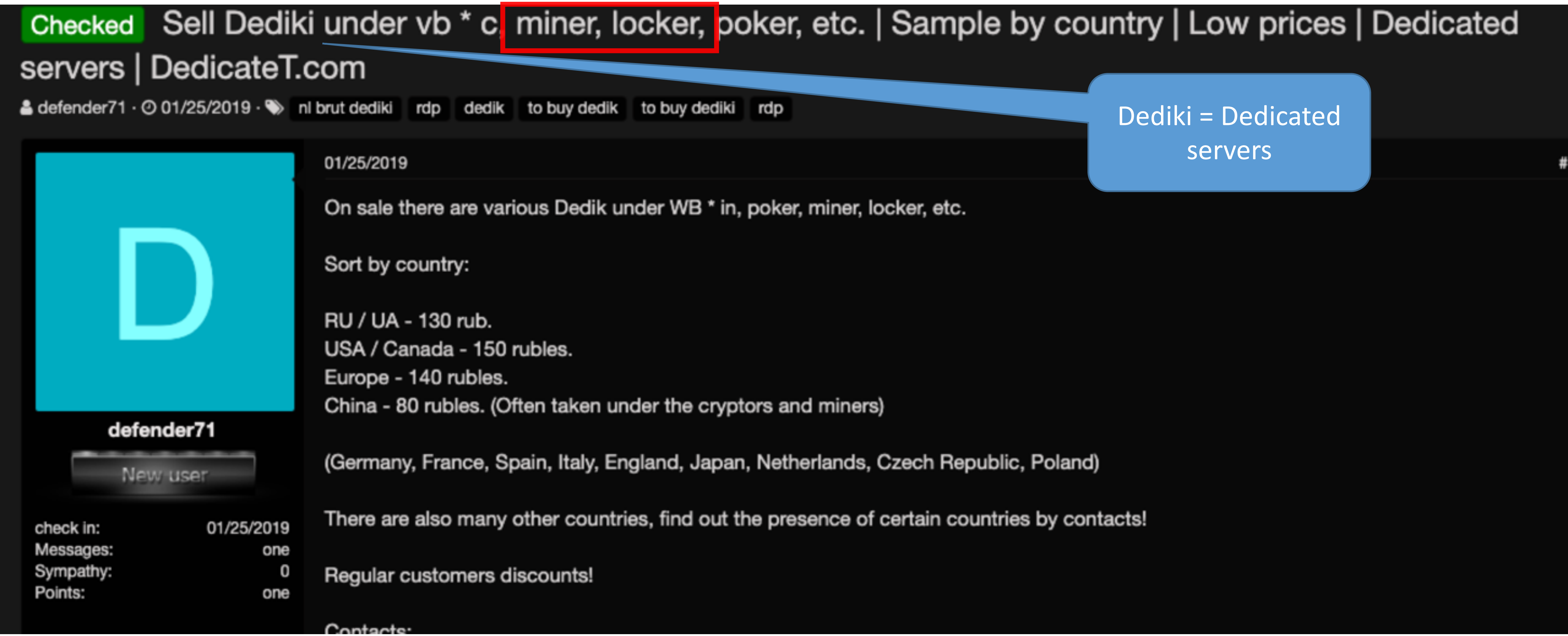
"We are not a ransomware that spreads automatic ally, we are professional hacker organization that specifically targets enterprises"

PlugX for ransom is not a single instance

- 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

Targeted ransomware and mining campaigns



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

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

Dediki = Dedicated servers

D

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)

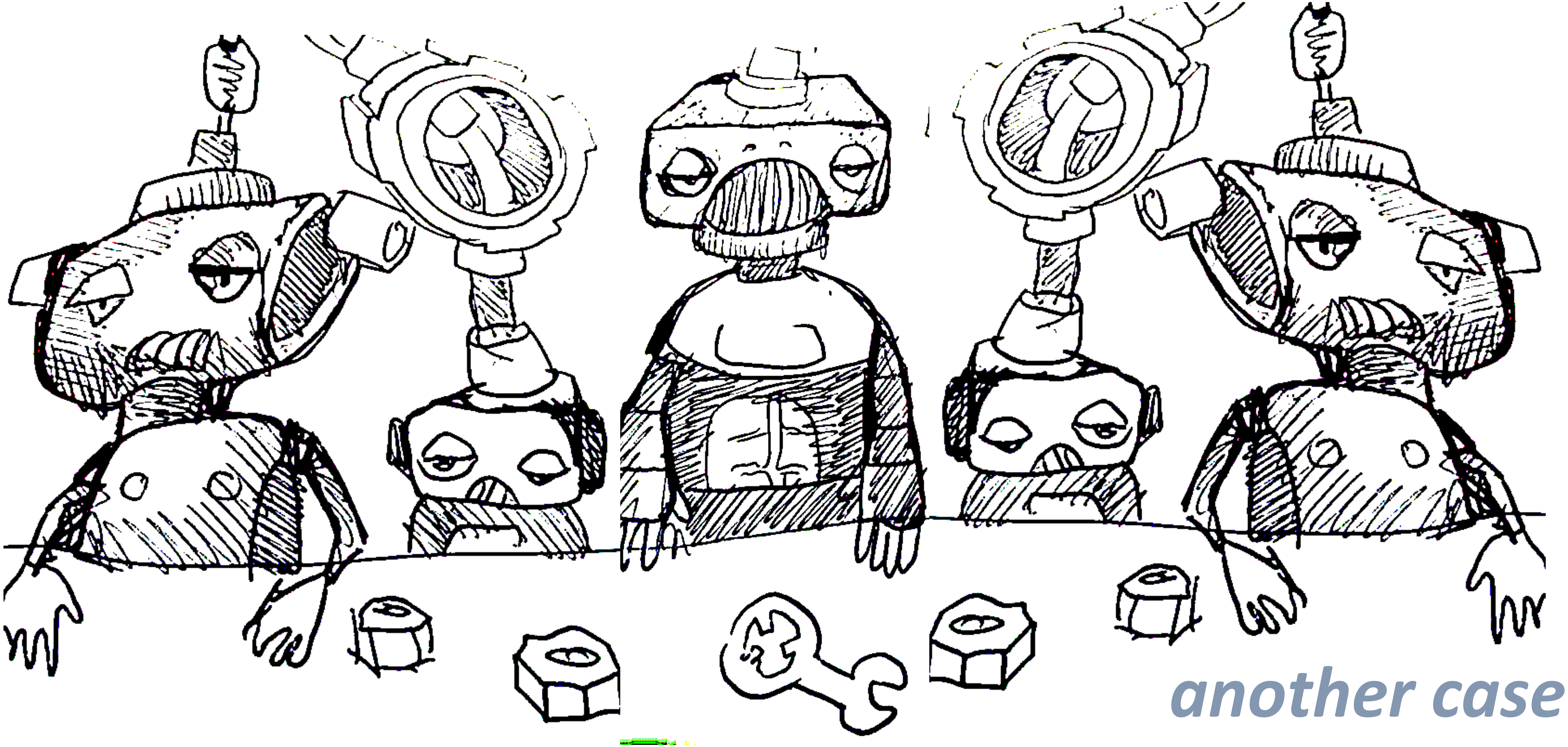
(Germany, France, Spain, Italy, England, Japan, Netherlands, Czech Republic, Poland)

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

Regular customers discounts!

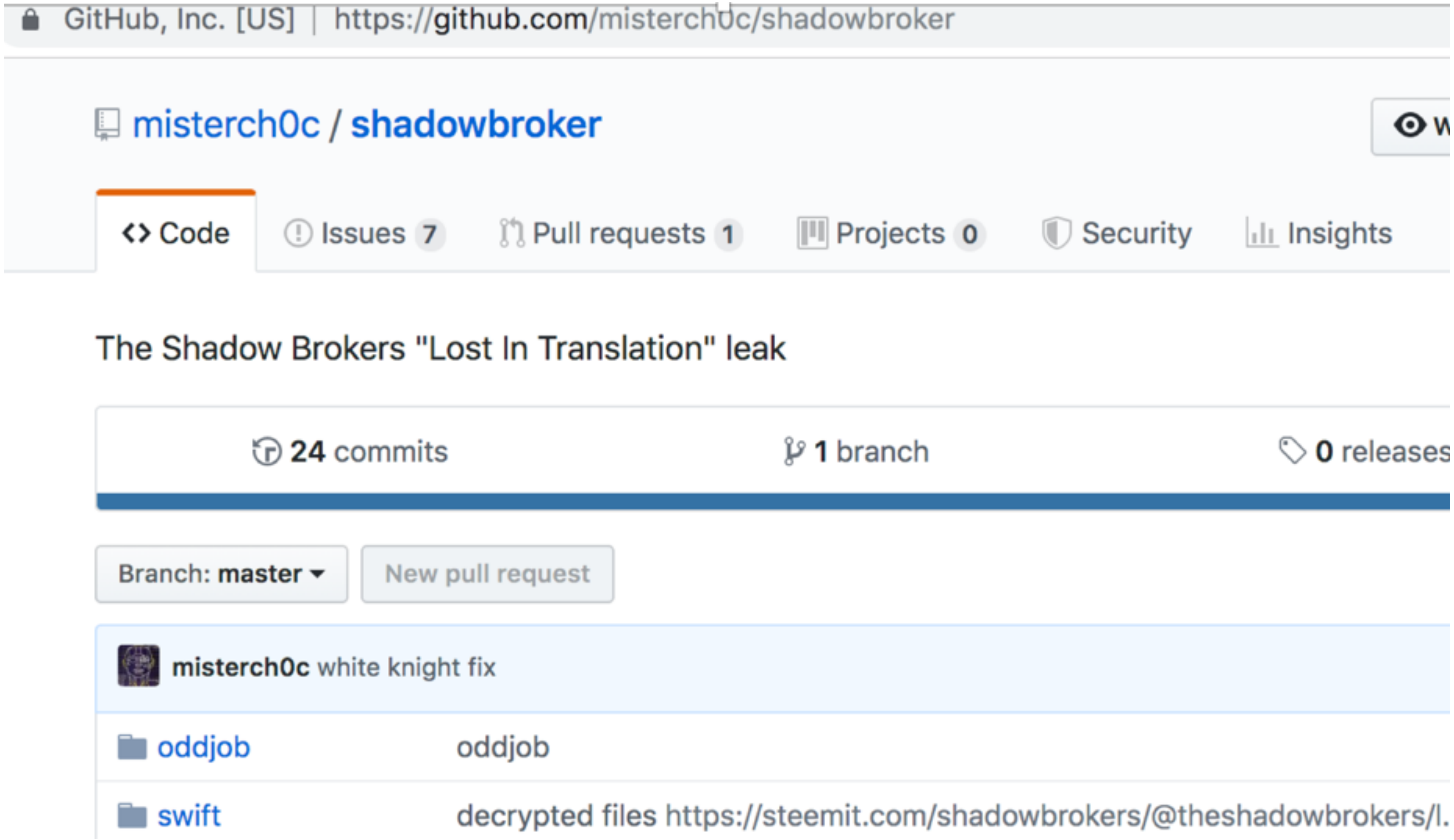
Contacts:

Strange things in Manufacturing Networks



another case

Equation tools weaponized to distribute coin miner



GitHub, Inc. [US] | https://github.com/misterch0c/shadowbroker

misterch0c / shadowbroker

The Shadow Brokers "Lost In Translation" leak

24 commits

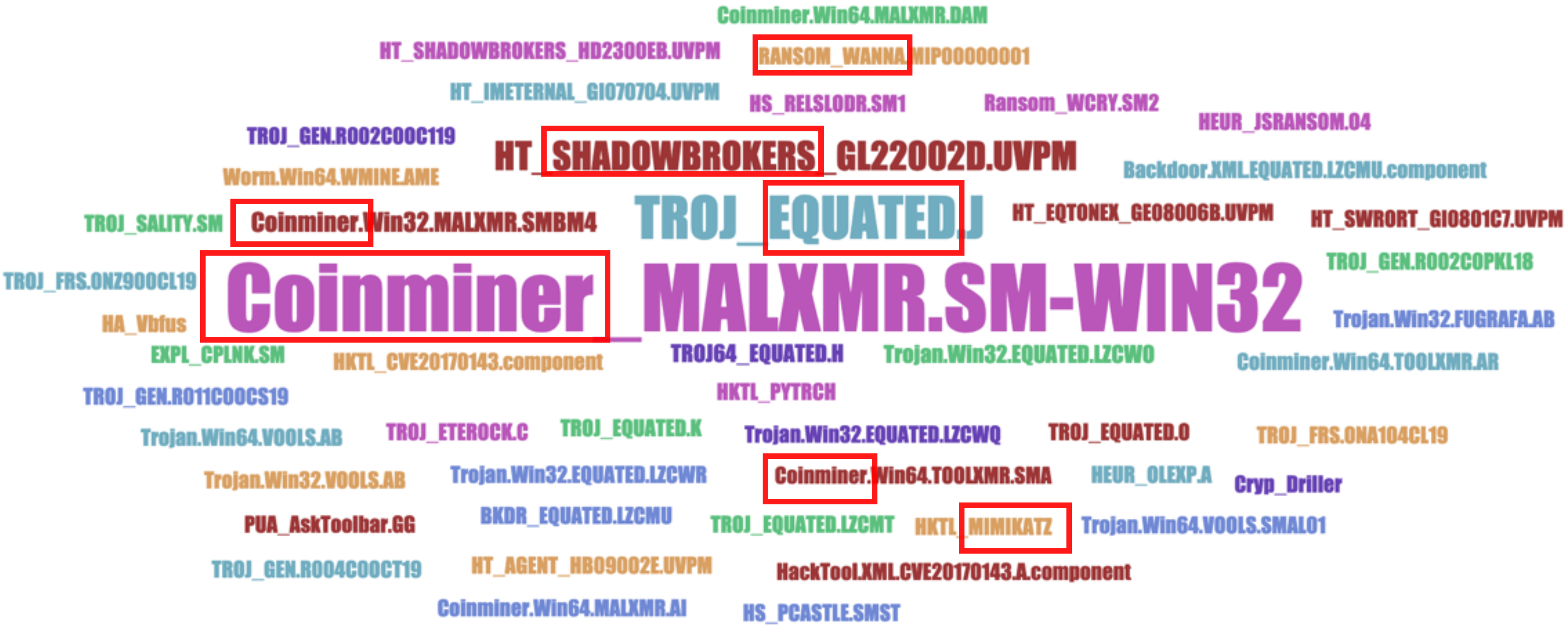
1 branch

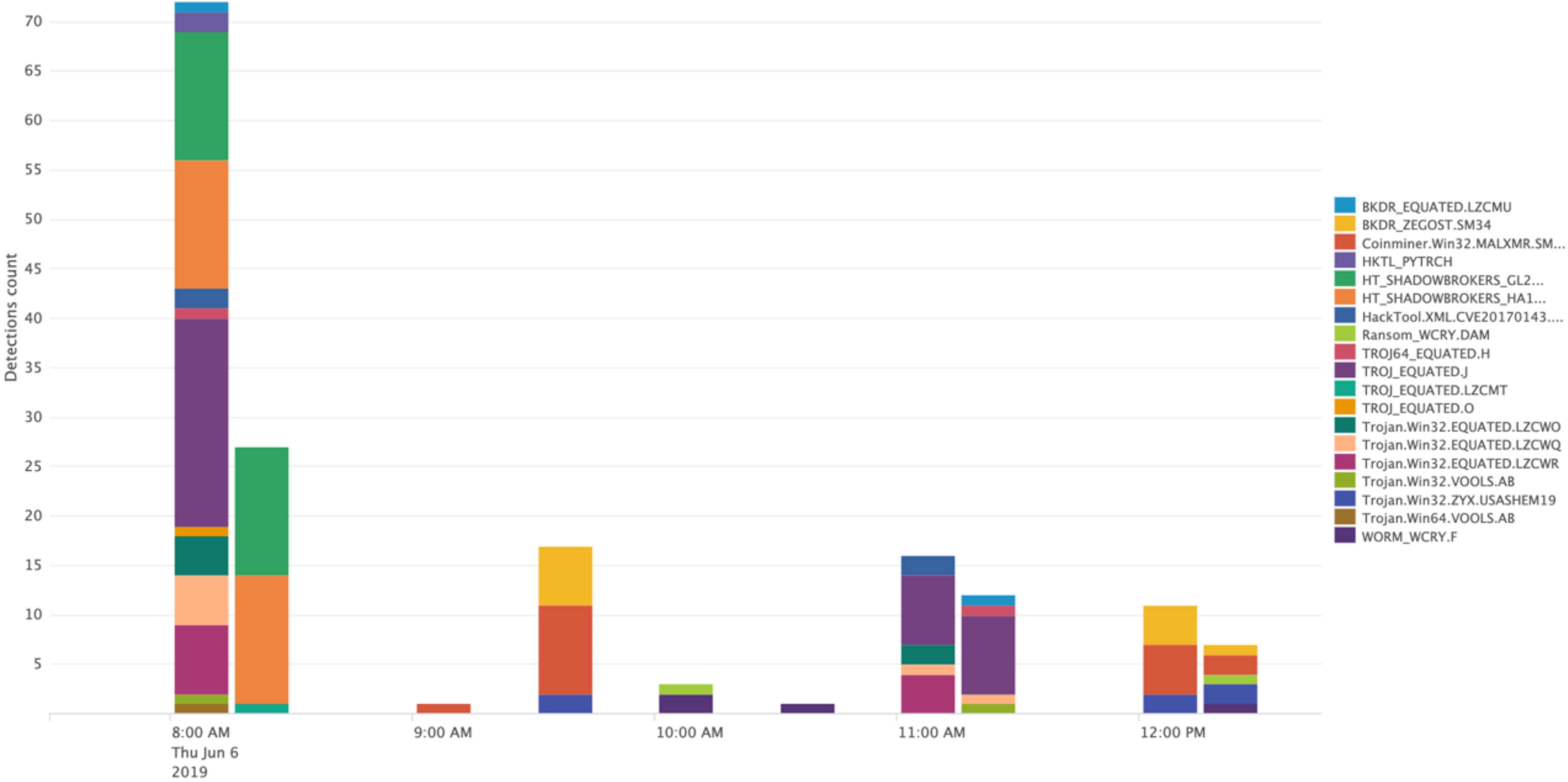
0 releases

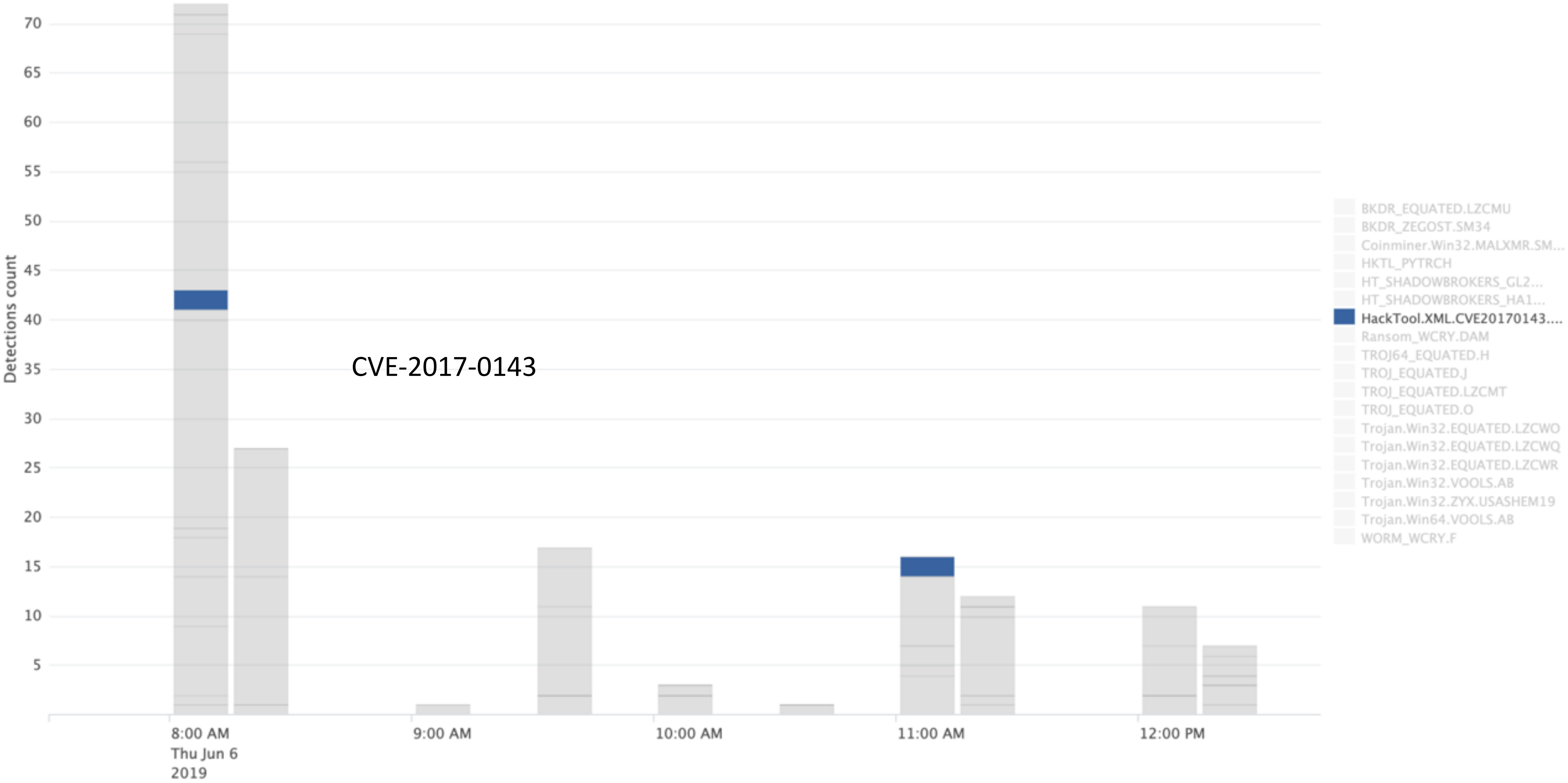
misterch0c white knight fix

oddjob	oddjob
swift	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l.

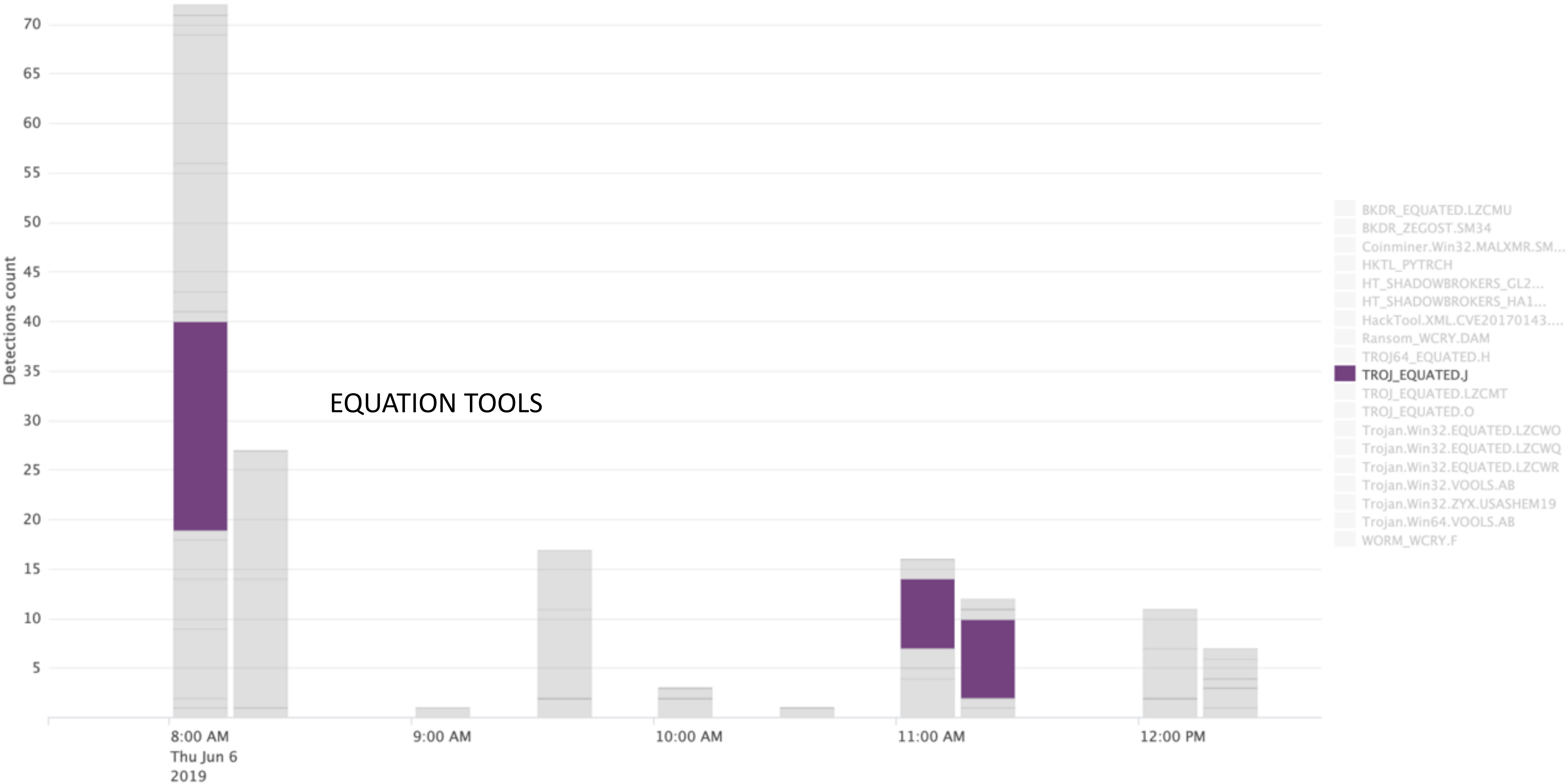
Snapshot of activity in the affected infrastructures




70
65
60
55
50
45
40
35
30
25
20
15
10
5
Detections count
8:00 AM
Thu Jun 6
2019
9:00 AM
10:00 AM
11:00 AM
12:00 PM
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

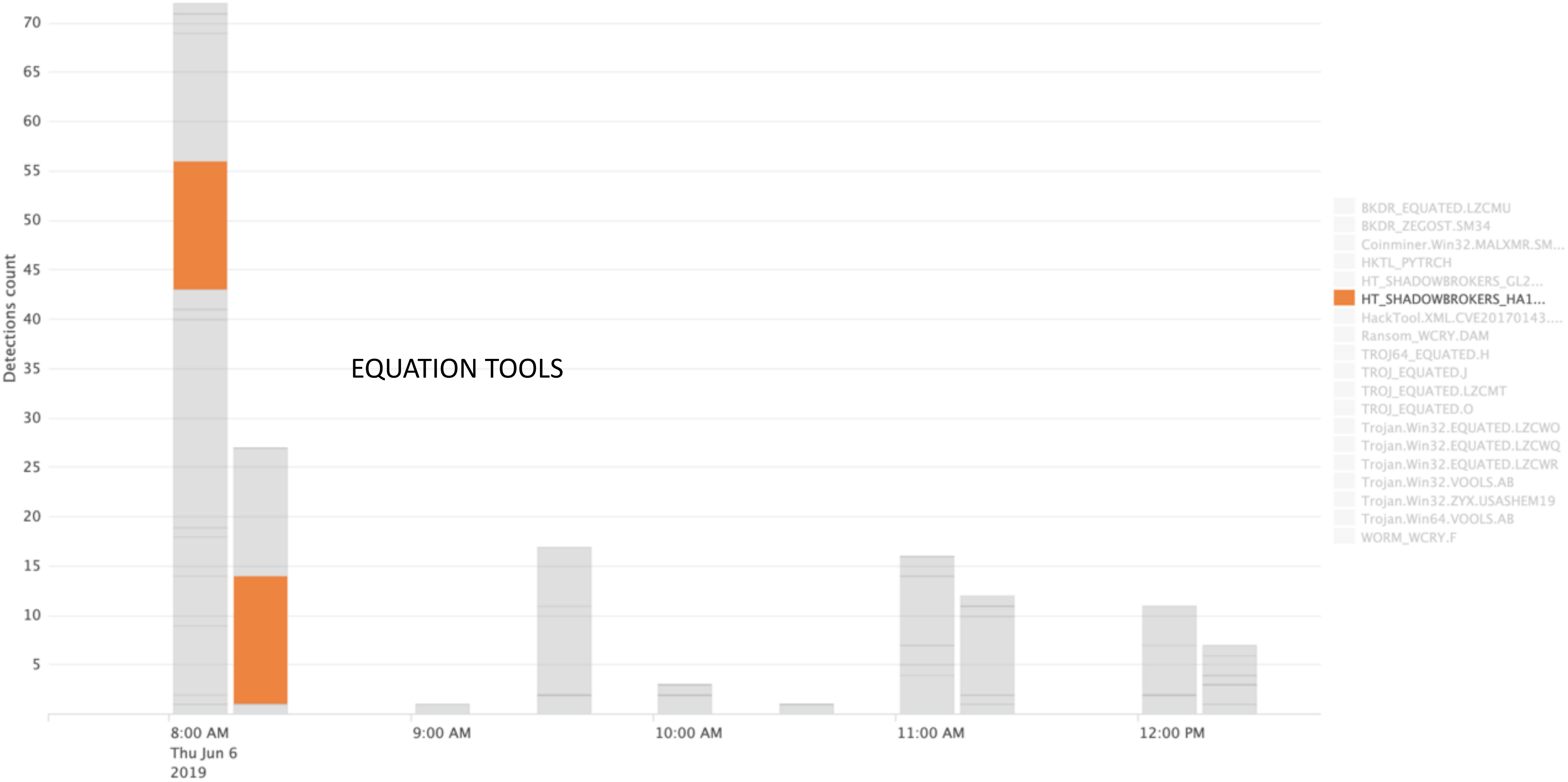


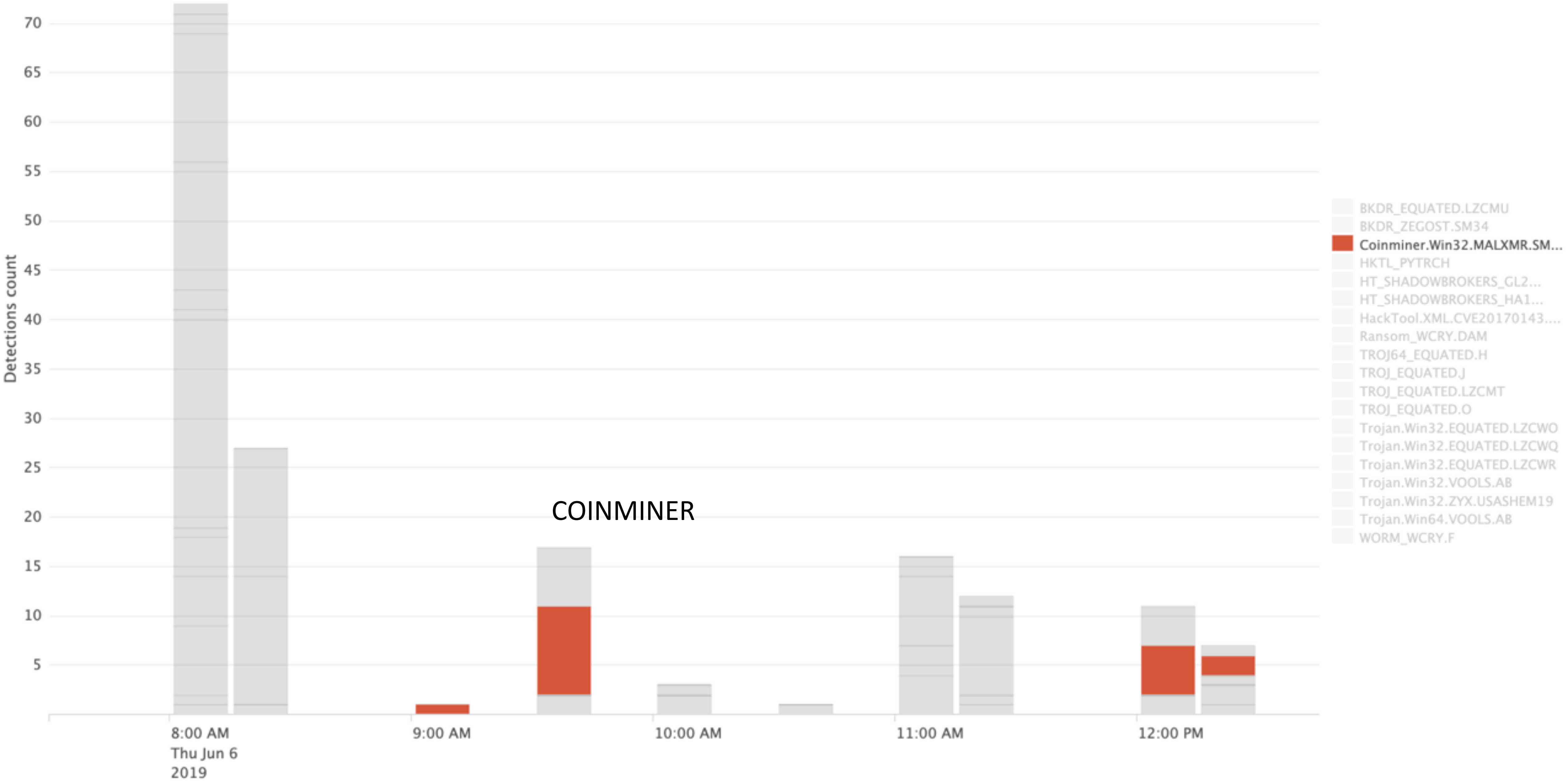
CVE-2017-0143



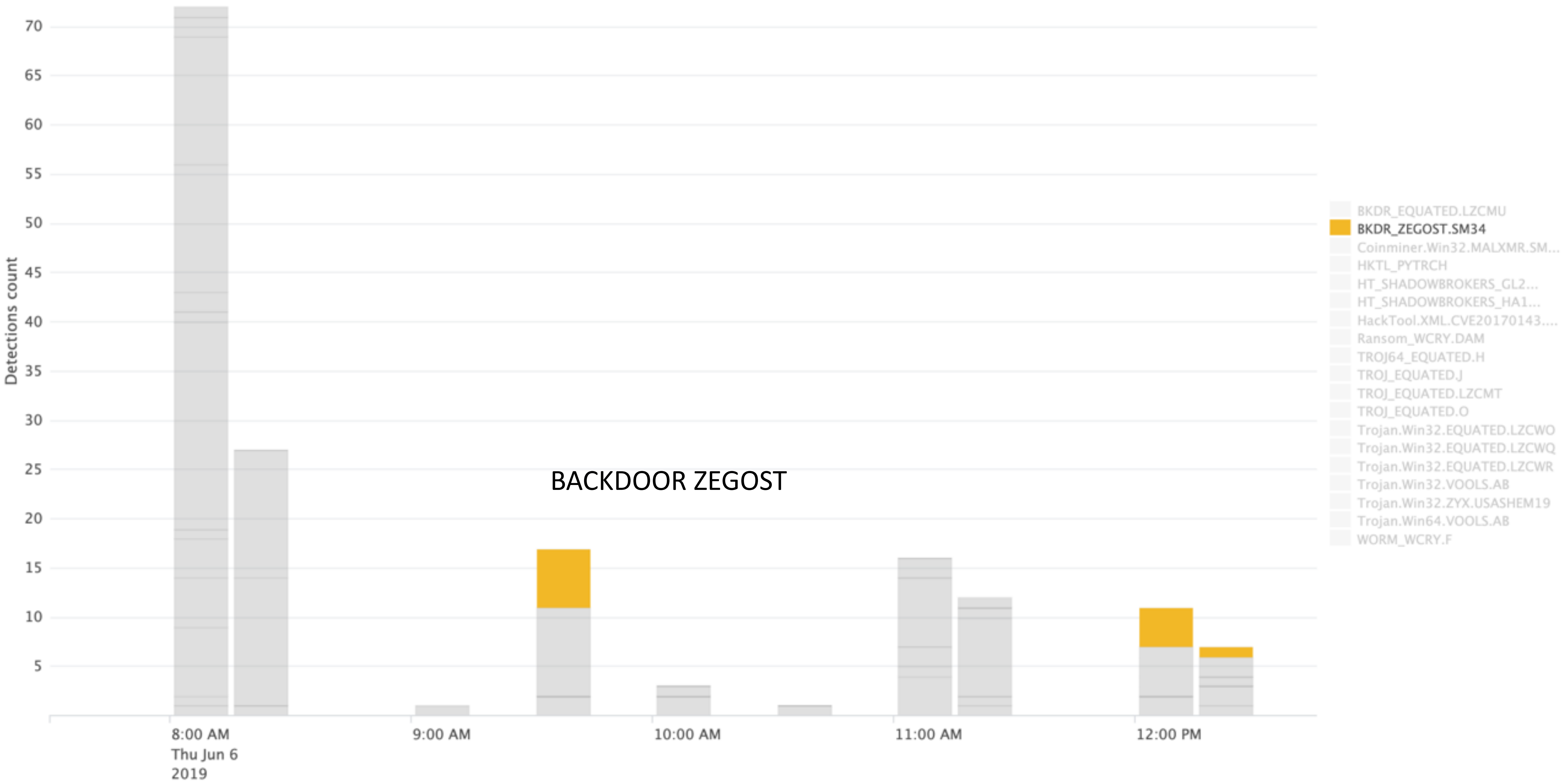
EQUATION TOOLS

EQUATION TOOLS




70
65
60
55
50
45
40
35
30
25
20
15
10
5
Detections count
8:00 AM
Thu Jun 6
2019
9:00 AM
10:00 AM
11:00 AM
12:00 PM
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

COINMINER



BACKDOOR ZEGOST

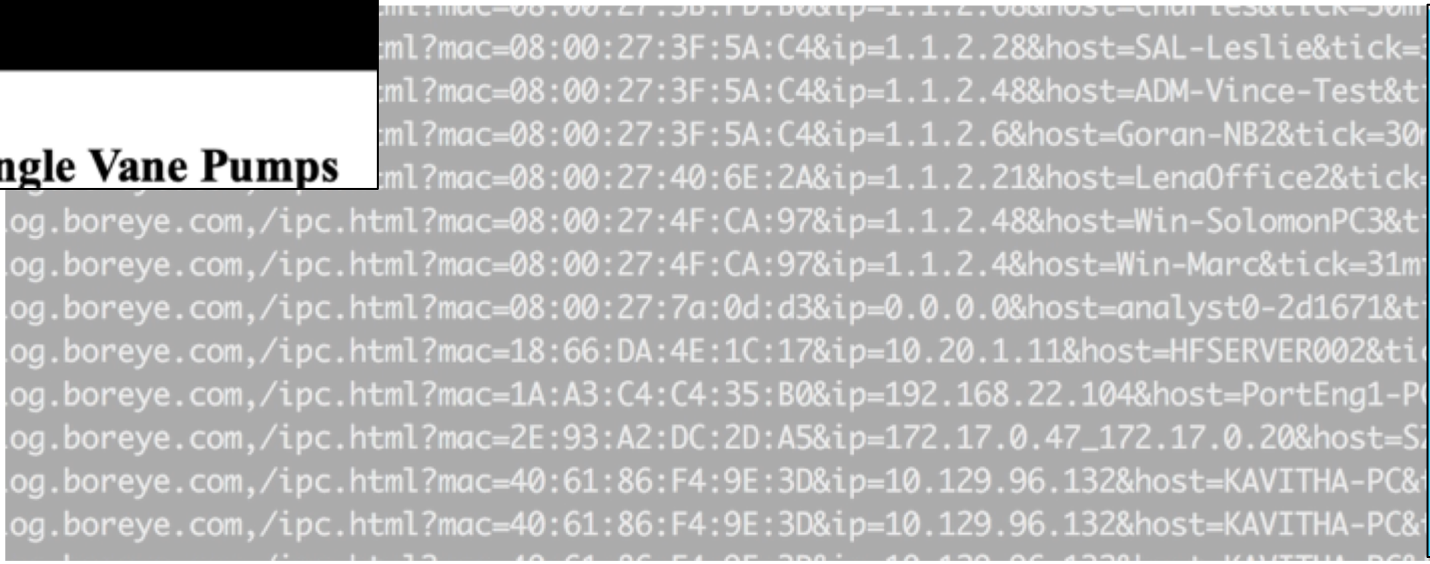
Possible insight on victim machines

- 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

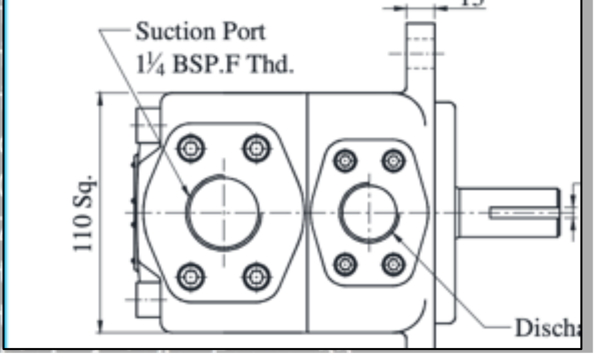


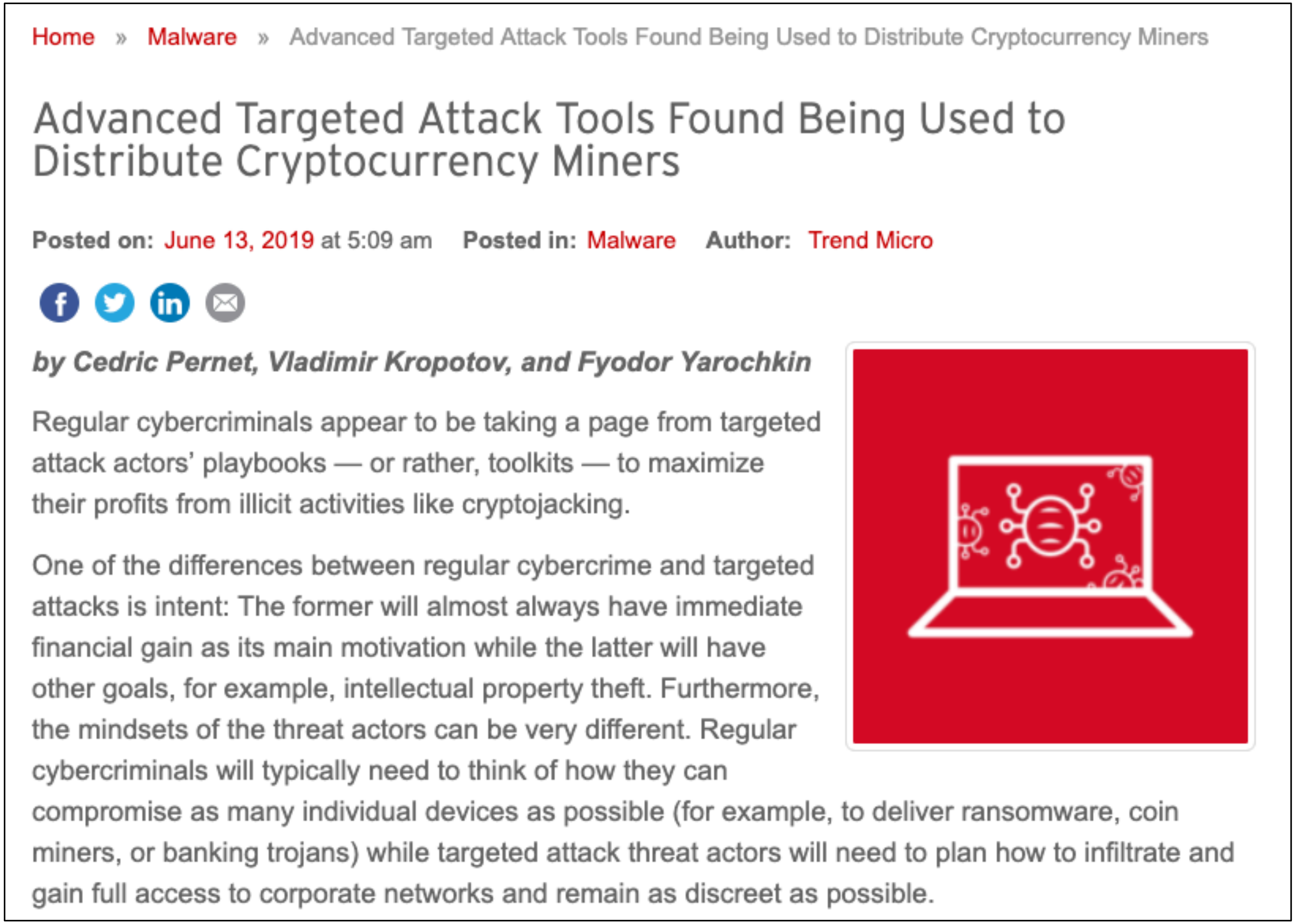
```
ml?mac=08:00:27:3B:FD:B0&ip=1.1.2.68&host=Charles&tick=30m
ml?mac=08:00:27:3F:5A:C4&ip=1.1.2.28&host=SAL-Leslie&tick=
ml?mac=08:00:27:3F:5A:C4&ip=1.1.2.48&host=ADM-Vince-Test&t
ml?mac=08:00:27:3F:5A:C4&ip=1.1.2.6&host=Goran-NB2&tick=30
ml?mac=08:00:27:40:6E:2A&ip=1.1.2.21&host=LenaOffice2&tick
og.boreye.com,/ipc.html?mac=08:00:27:4F:CA:97&ip=1.1.2.48&host=Win-SolomonPC3&t
og.boreye.com,/ipc.html?mac=08:00:27:4F:CA:97&ip=1.1.2.4&host=Win-Marc&tick=31m
og.boreye.com,/ipc.html?mac=08:00:27:7a:0d:d3&ip=0.0.0.0&host=analyst0-2d1671&t
og.boreye.com,/ipc.html?mac=18:66:DA:4E:1C:17&ip=10.20.1.11&host=HFSERVER002&ti
og.boreye.com,/ipc.html?mac=1A:A3:C4:C4:35:B0&ip=192.168.22.104&host=PortEng1-P
og.boreye.com,/ipc.html?mac=2E:93:A2:DC:2D:A5&ip=172.17.0.47_172.17.0.20&host=S
og.boreye.com,/ipc.html?mac=40:61:86:F4:9E:3D&ip=10.129.96.132&host=KAVITHA-PC&
og.boreye.com,/ipc.html?mac=40:61:86:F4:9E:3D&ip=10.129.96.132&host=KAVITHA-PC&
```

YUKEN

■ PVR50-F-※-※-※※※-3180

- Flange Mounting





Home » Malware » Advanced Targeted Attack Tools Found Being Used to Distribute Cryptocurrency Miners

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

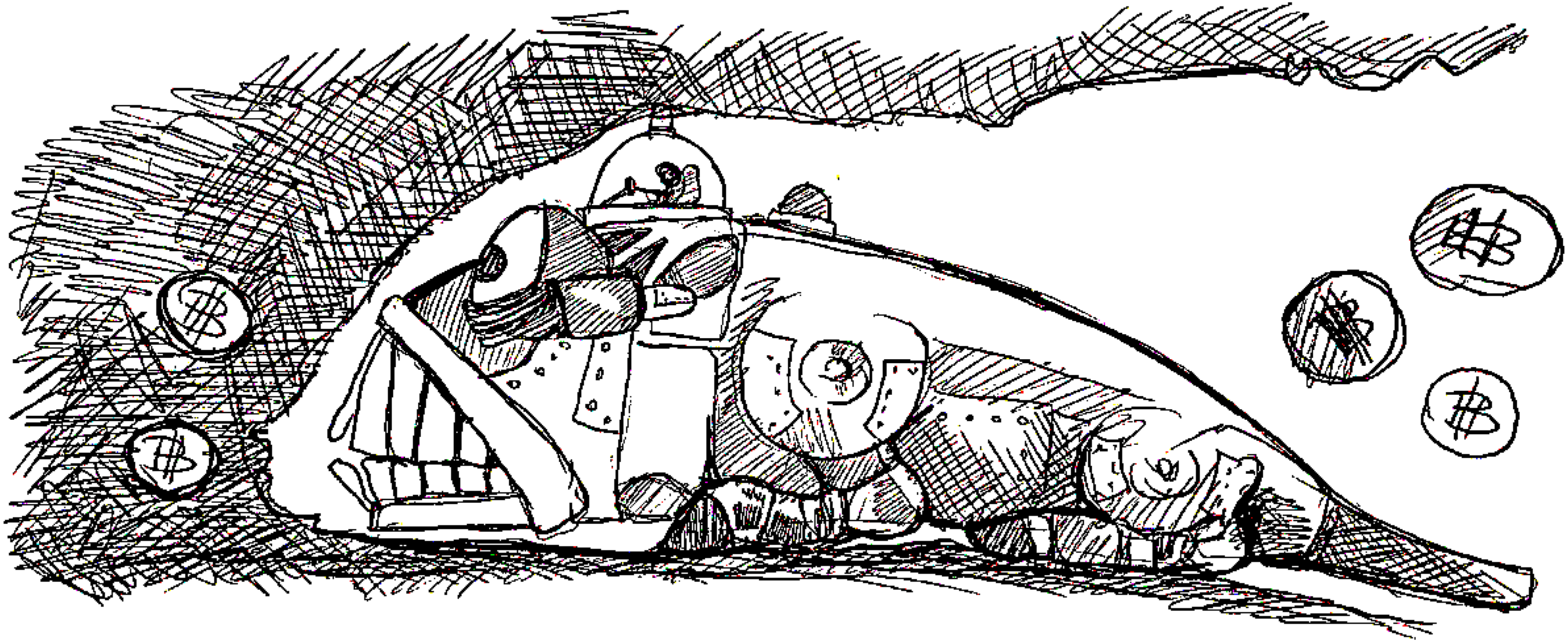
by Cedric Pernet, Vladimir Kropotov, and Fyodor Yarochkin

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.

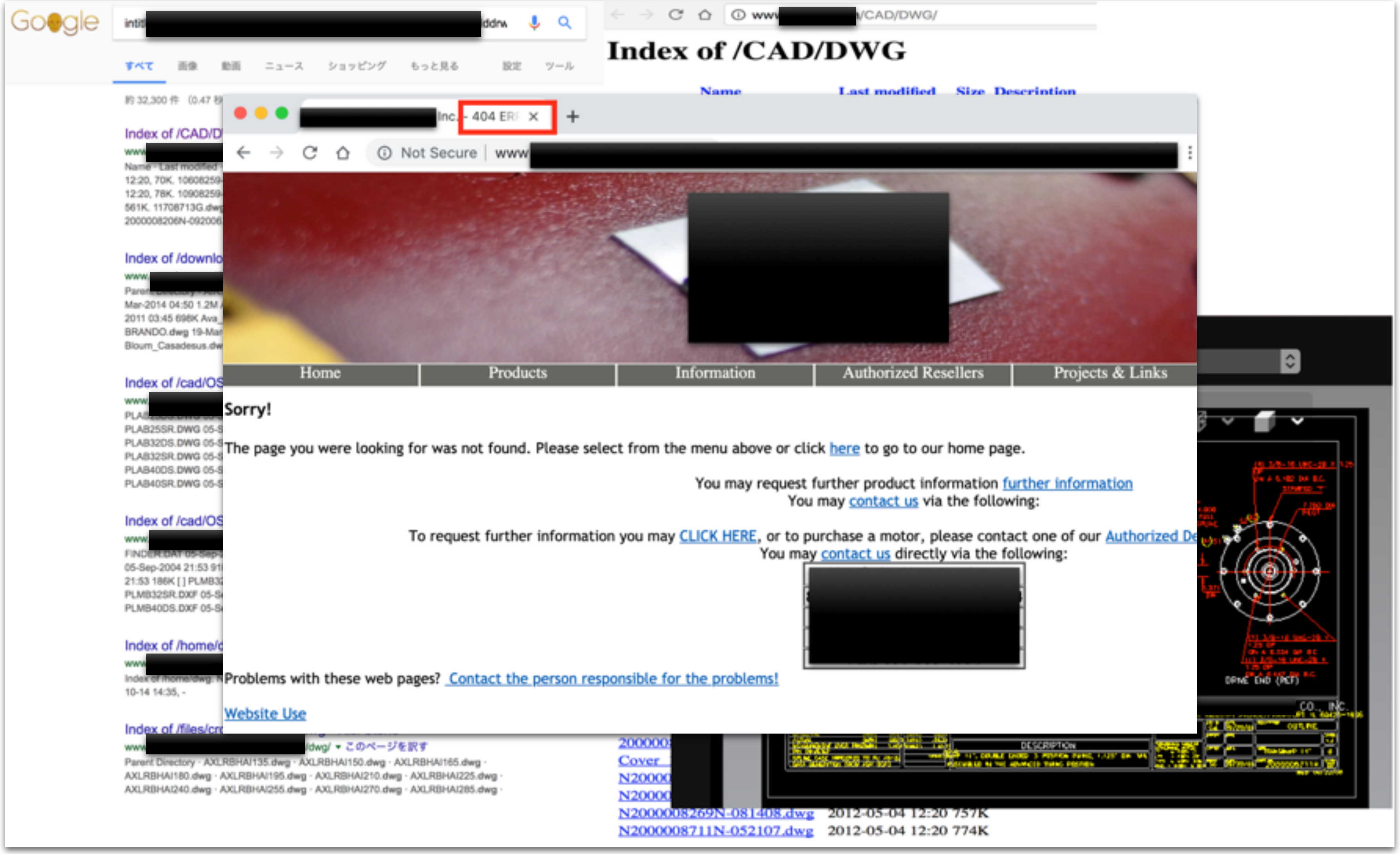
https://blog.trendmicro.com/trendlabs-security-intelligence/advanced-targeted-attack-tools-used-to-distribute-cryptocurrency-miners/

APT tools For Coin mining and Ransom



Threats and Risks to Intellectual Property

Unintentional leaks due to poor configuration



intitl [redacted] ddrw

すべて 画像 動画 ニュース ショッピング もっと見る 設定 ツール

約 32,300 件 (0.47 秒

Index of /CAD/D

www [redacted]

Name · Last modified
12:20, 70K. 10608259
12:20, 78K. 10908259
561K. 11708713G.dwg
2000008206N-092006

Index of /downlo

www [redacted]

Parent Directory
Mar-2014 04:50 1.2M
2011 03:45 698K Ava_
BRANDO.dwg 19-Mar
Bloum_Casadesus.dw

Index of /cad/OS

www [redacted]

PLA
PLAB25SR.DWG 05-S
PLAB32DS.DWG 05-S
PLAB32SR.DWG 05-S
PLAB40DS.DWG 05-S
PLAB40SR.DWG 05-S

Index of /cad/OS

www [redacted]

FINDER.DAT 05-Sep-
05-Sep-2004 21:53 91
21:53 186K [ ] PLMB32
PLMB32SR.DXF 05-S
PLMB40DS.DXF 05-S

Index of /home/d

www [redacted]

Index of /home/dwg: N
10-14 14:35, -

Index of /files/cr

www [redacted] /dwg/ ▾ このページを訳す

Parent Directory · AXLRBHAI135.dwg · AXLRBHAI150.dwg · AXLRBHAI165.dwg · AXLRBHAI180.dwg · AXLRBHAI195.dwg · AXLRBHAI210.dwg · AXLRBHAI225.dwg · AXLRBHAI240.dwg · AXLRBHAI255.dwg · AXLRBHAI270.dwg · AXLRBHAI285.dwg ·

[redacted] Inc. - 404 ERR ×

Not Secure | www [redacted]

[redacted]

Sorry!

The page you were looking for was not found. Please select from the menu above or click here to go to our home page.

You may request further product information further information
You may contact us via the following:

To request further information you may CLICK HERE, or to purchase a motor, please contact one of our Authorized De
You may contact us directly via the following:

[redacted]

Problems with these web pages? Contact the person responsible for the problems!

Website Use

ww [redacted] /CAD/DWG/

Index of /CAD/DWG

Name	Last modified	Size	Description
200000			
Cover			
N20000			
N20000			
N2000008269N-081408.dwg	2012-05-04 12:20	757K	
N2000008711N-052107.dwg	2012-05-04 12:20	774K	

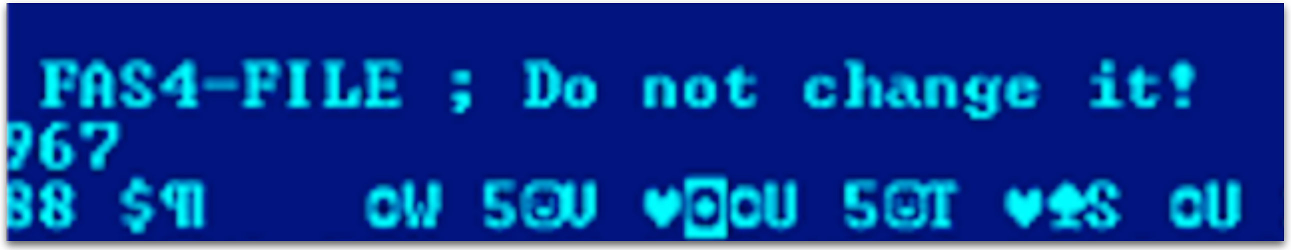
Malicious CAD files

ACM_SHENZ.A

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

ACM_MEDRE.AA

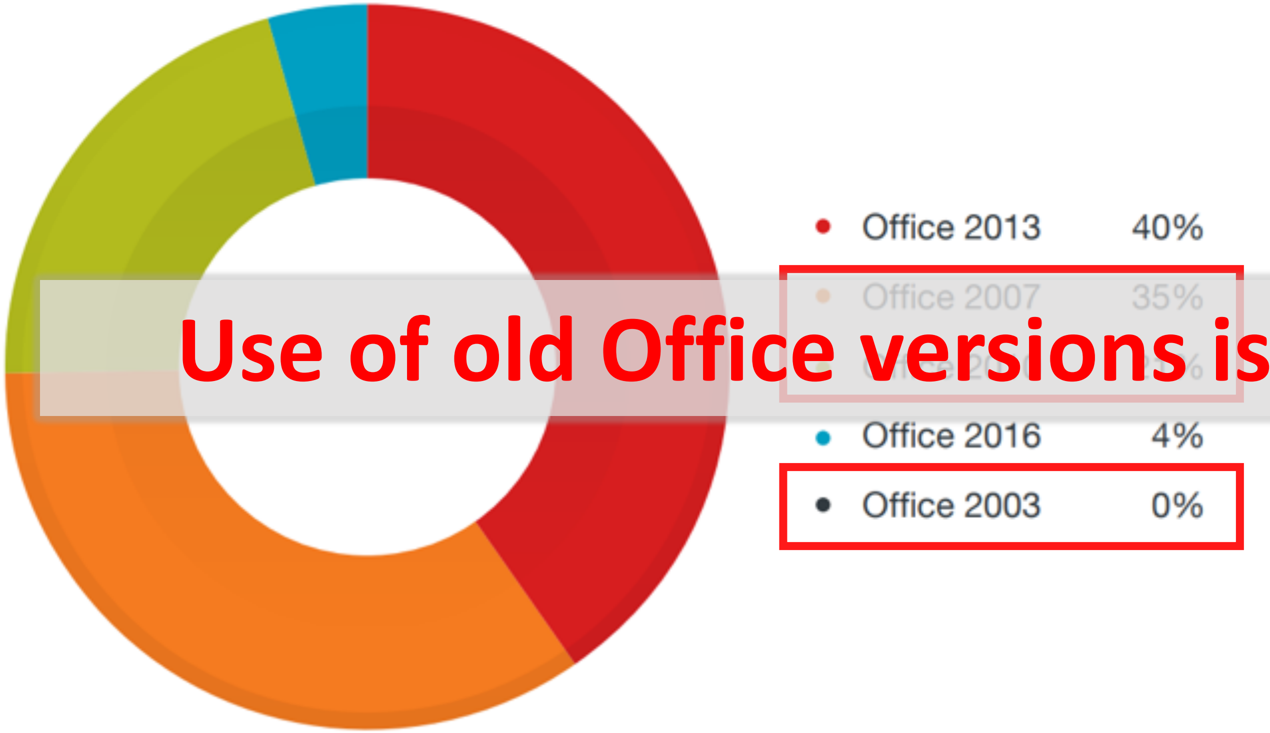
- Send PST file of Microsoft Outlook to a predefined email address
- Send an opened CAD (DWG) file to a predefined email address



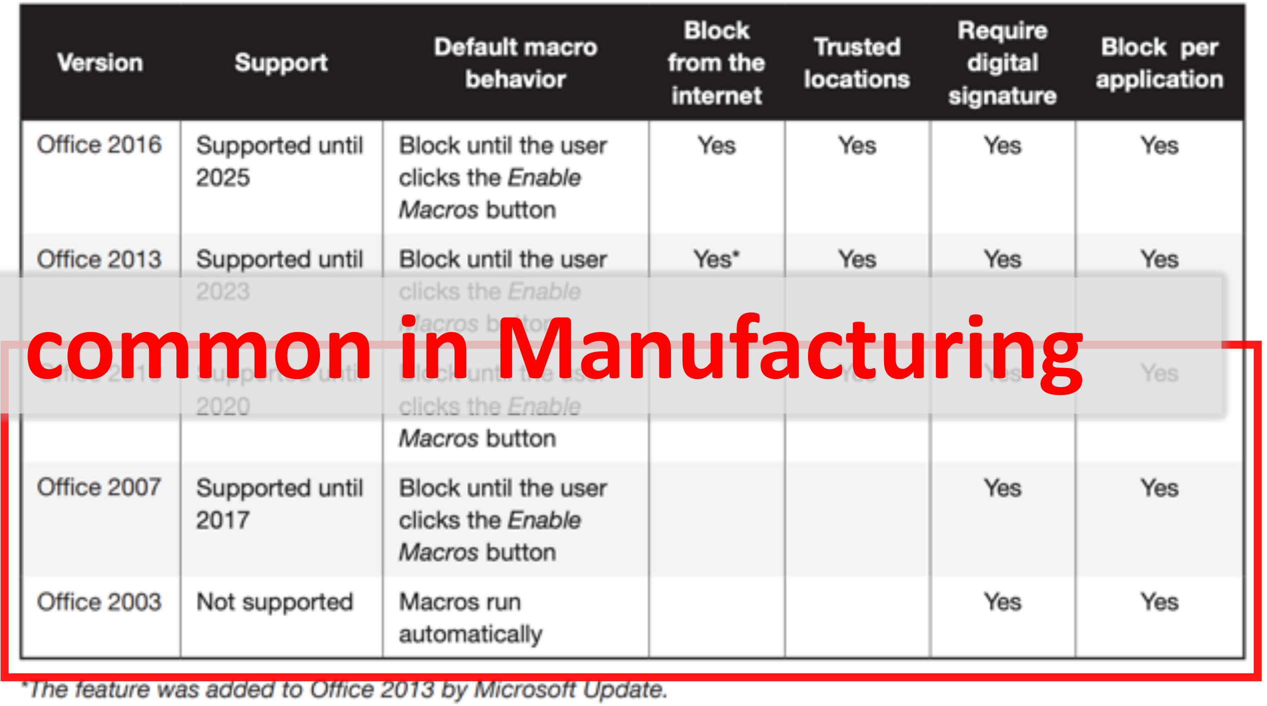
```
FAS4-FILE ; Do not change it!
967
88 $¶       oW 5☺U ♥▣oU 5☺T ♥♠S oU
```

CAD file can be weaponized for espionage

Use of older version of Microsoft Office



Use of old Office versions is common in Manufacturing



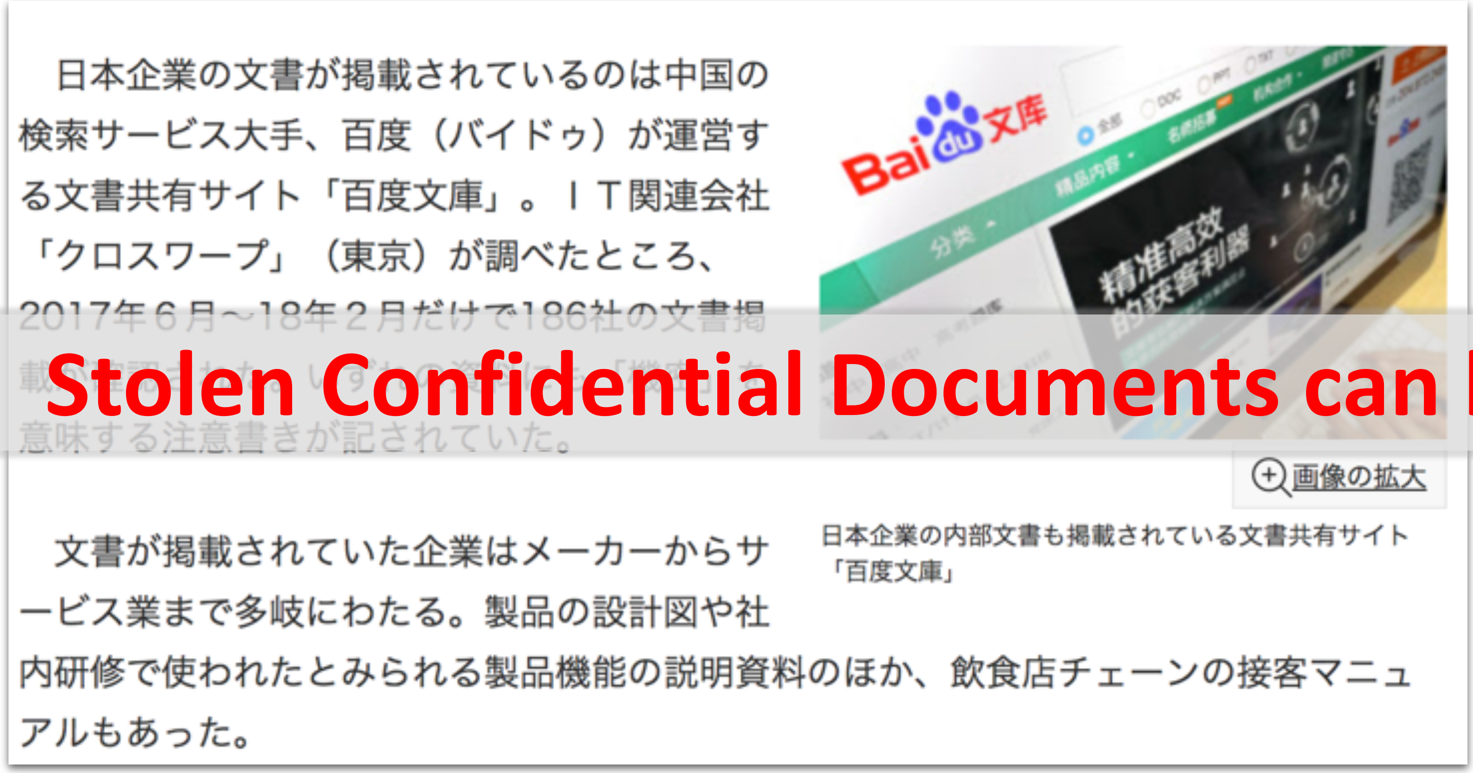
Version	Support	Default macro behavior	Block from the internet	Trusted locations	Require digital signature	Block per application
Office 2016	Supported until 2025	Block until the user clicks the *Enable Macros* button	Yes	Yes	Yes	Yes
Office 2013	Supported until 2023	Block until the user clicks the *Enable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

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

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



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。

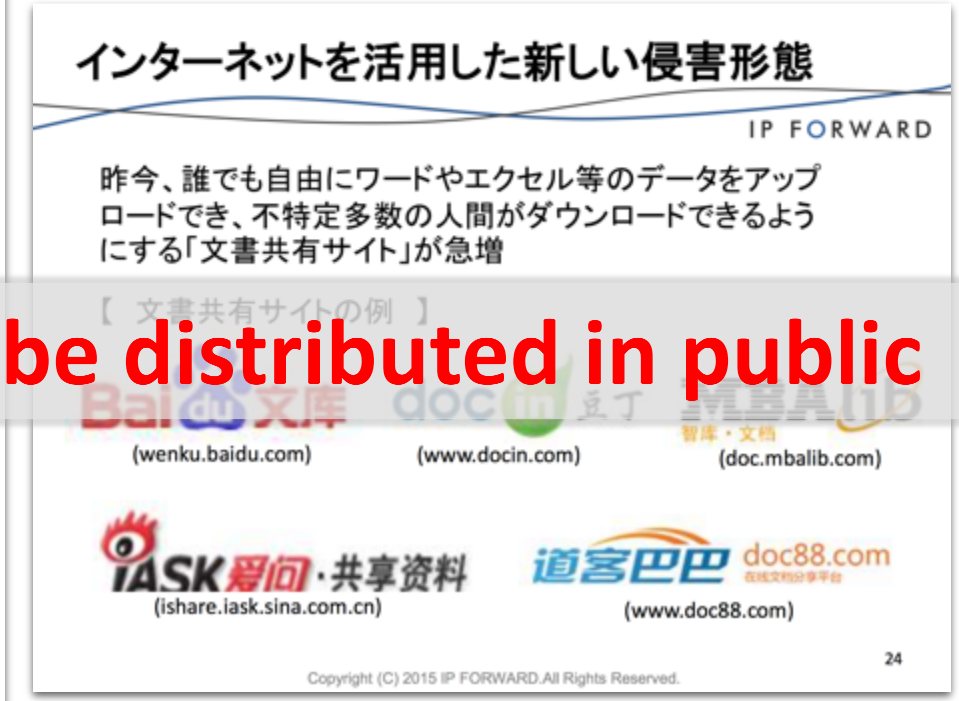
画像の拡大

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」

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/DGXMZO27564530010320 18CR8000/

Stolen Confidential Documents can be distributed in public



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する「文書共有サイト」が急増

【　文書共有サイトの例　】

(wenku.baidu.com)　(www.docin.com)　(doc.mbalib.com)

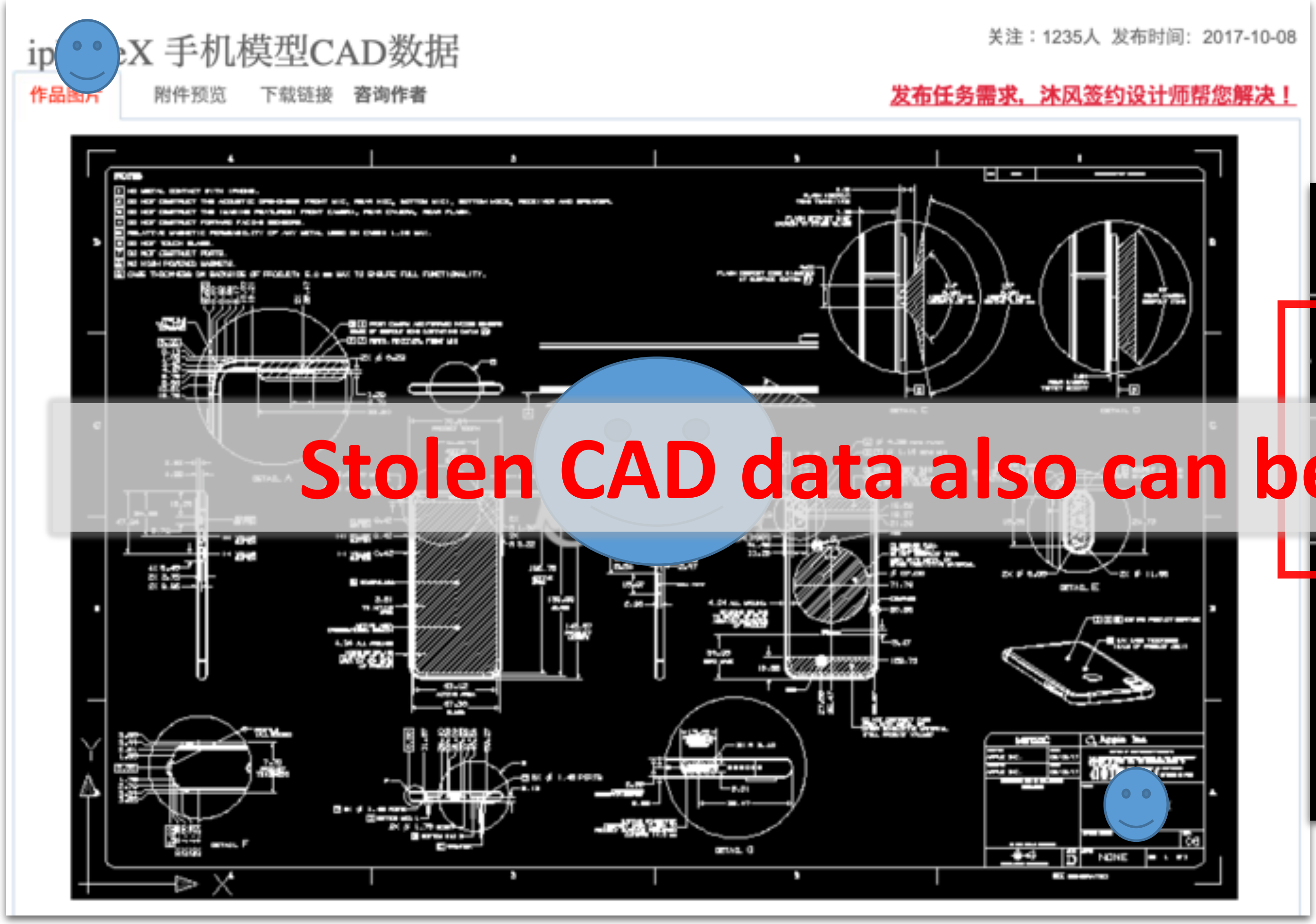
(ishare.iask.sina.com.cn)　(www.doc88.com)

24

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

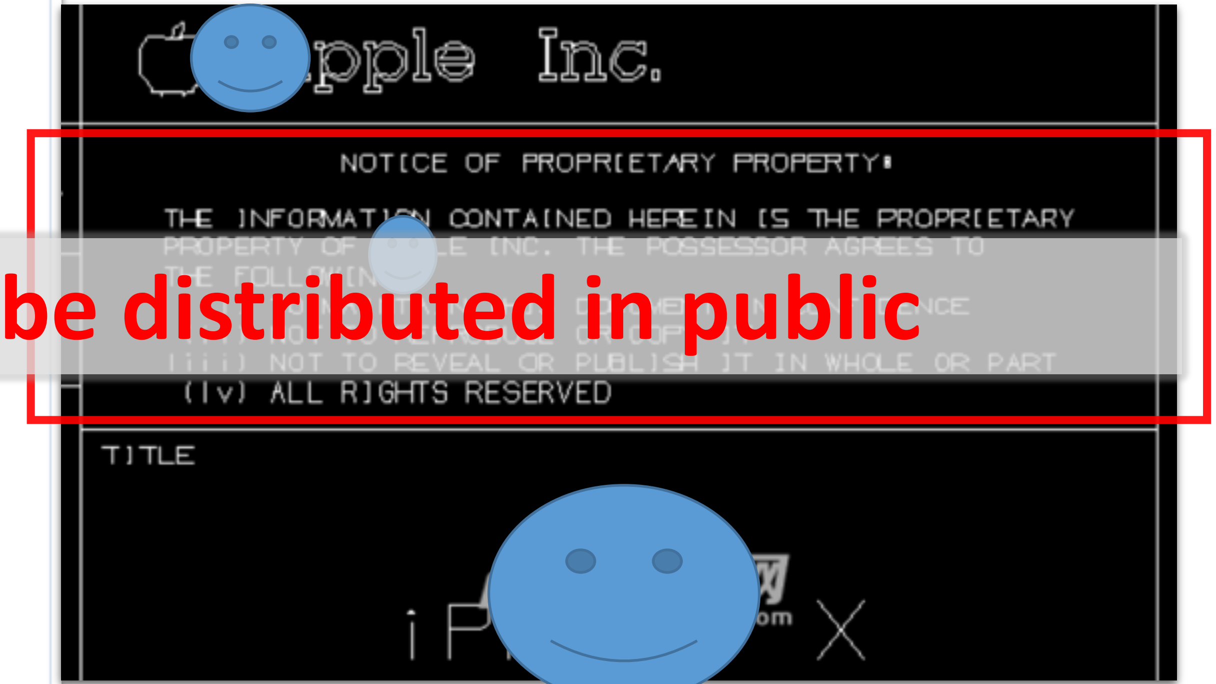


ip[redacted]eX 手机模型CAD数据

关注：1235人 发布时间：2017-10-08

[redacted] 附件预览 下载链接 咨询作者

发布任务需求，沐风签约设计师帮您解决！



[redacted]pple Inc.

NOTICE OF PROPRIETARY PROPERTY:

THE INFORMATION CONTAINED HEREIN IS THE PROPRIETARY PROPERTY OF [redacted]LE INC. THE POSSESSOR AGREES TO THE FOLLOWIN[redacted]

(iii) NOT TO REVEAL OR PUBLISH IT IN WHOLE OR PART

(iv) ALL RIGHTS RESERVED

TITLE

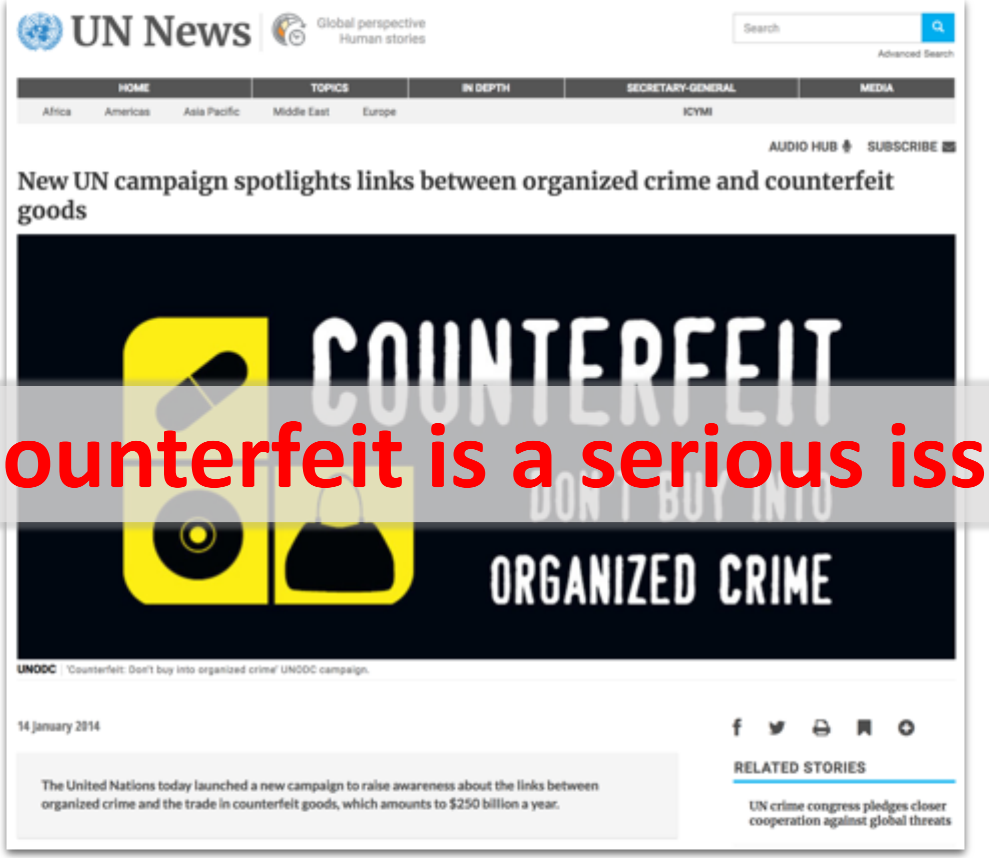
iP[redacted] X

Stolen CAD data also can be distributed in public

Sites showing leaked CAD files pertaining to a popular smartphone

Counterfeit products issue

Counterfeit is a serious issue for Manufacturing companies



New UN campaign spotlights links between organized crime and counterfeit goods

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

14 January 2014

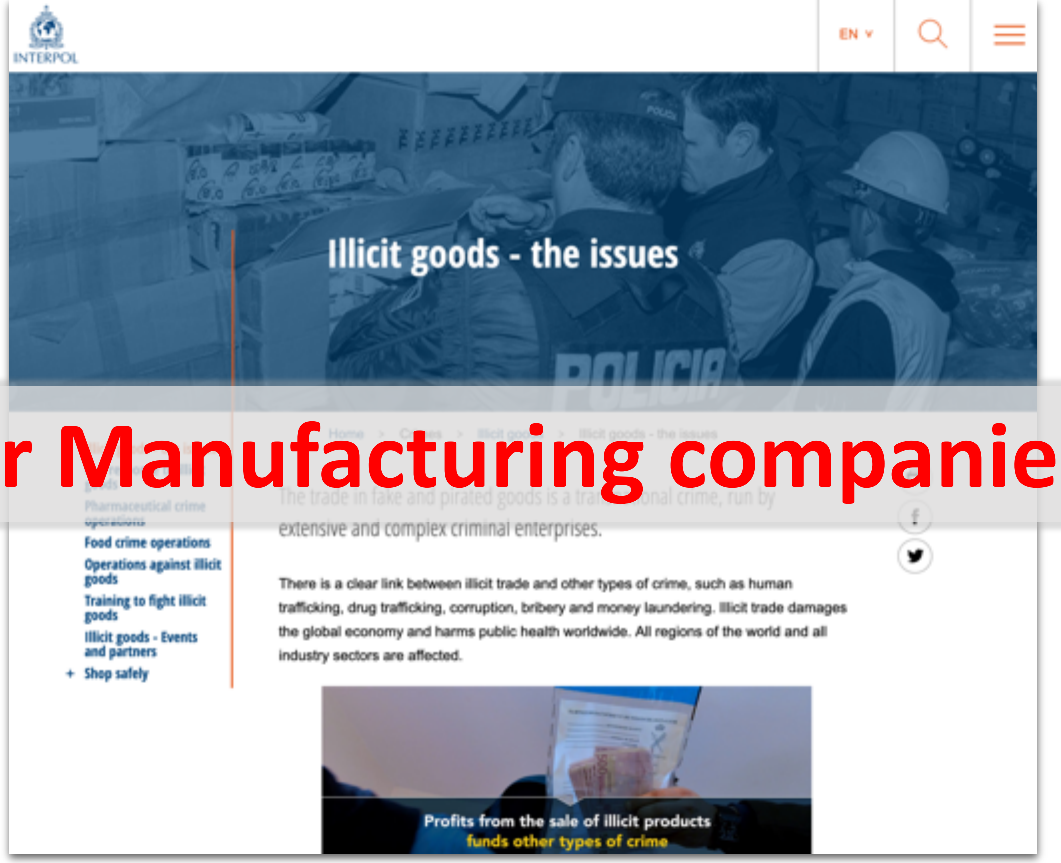
The United Nations today launched a new campaign to raise awareness about the links between organized crime and the trade in counterfeit goods, which amounts to $250 billion a year.

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
Illicit goods - the issues
POLICIA
Home > Crimes > Illicit goods > Illicit goods - the issues
Pharmaceutical crime operations
Food crime operations
Operations against illicit goods
Training to fight illicit goods
Illicit goods - Events and partners
+ Shop safely
Profits from the sale of illicit products
funds other types of crime

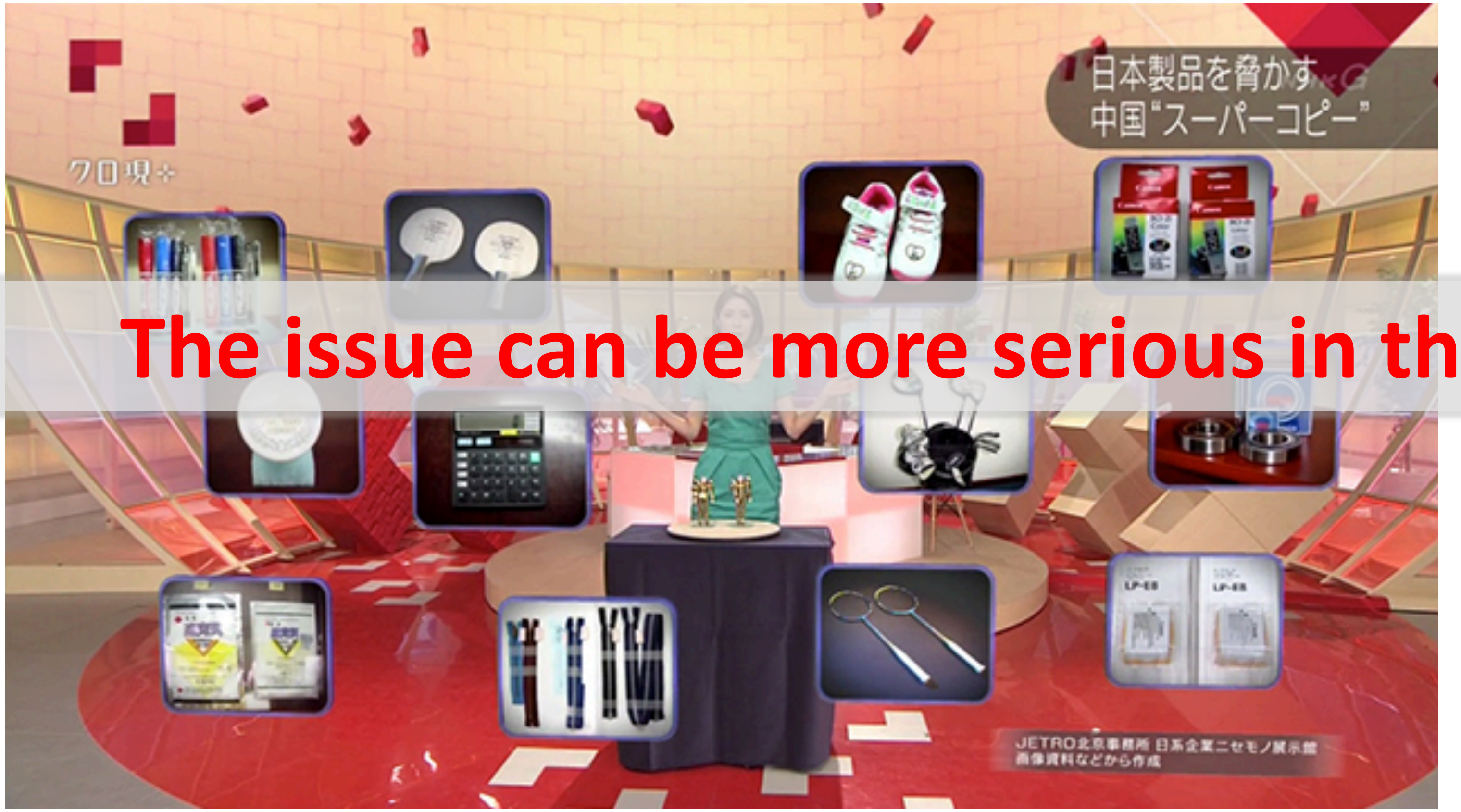
The trade in fake and pirated goods is a tra[illegible]onal crime, run by extensive and complex criminal enterprises.

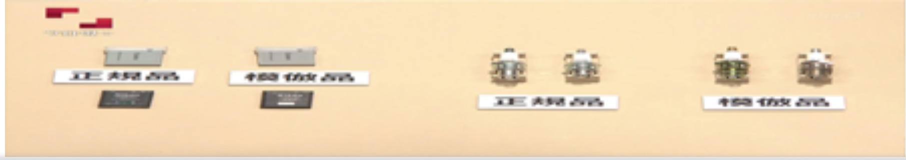
There is a clear link between illicit trade and other types of crime, such as human trafficking, drug trafficking, corruption, bribery and money laundering. Illicit trade damages the global economy and harms public health worldwide. All regions of the world and all industry sectors are affected.

One of major crimes for INTERPOL

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

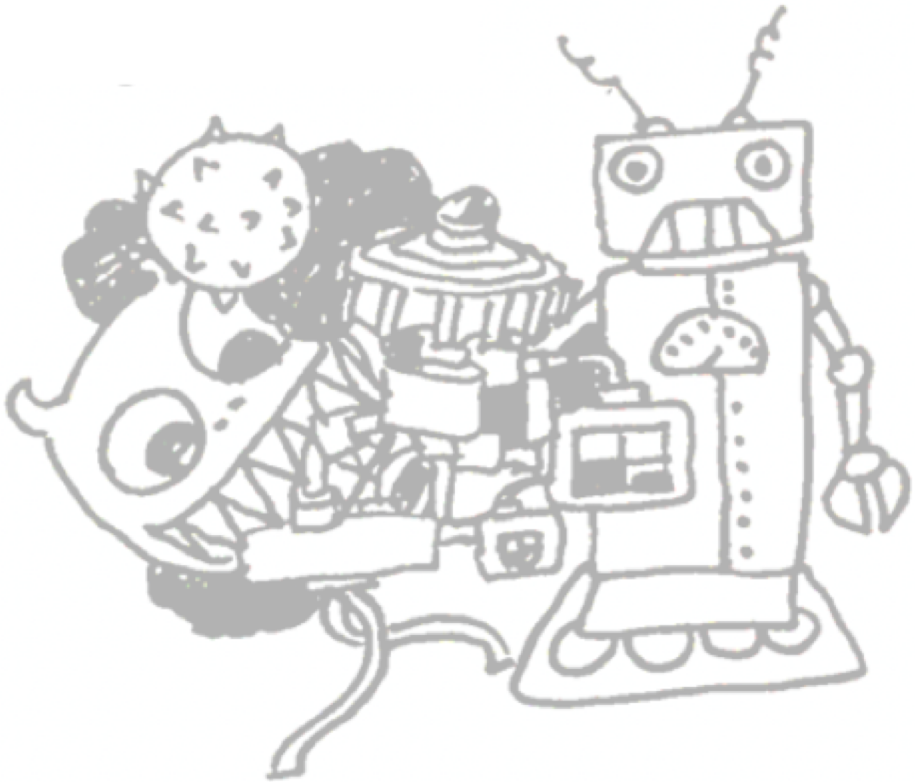
Counterfeit becomes “Supercopy”





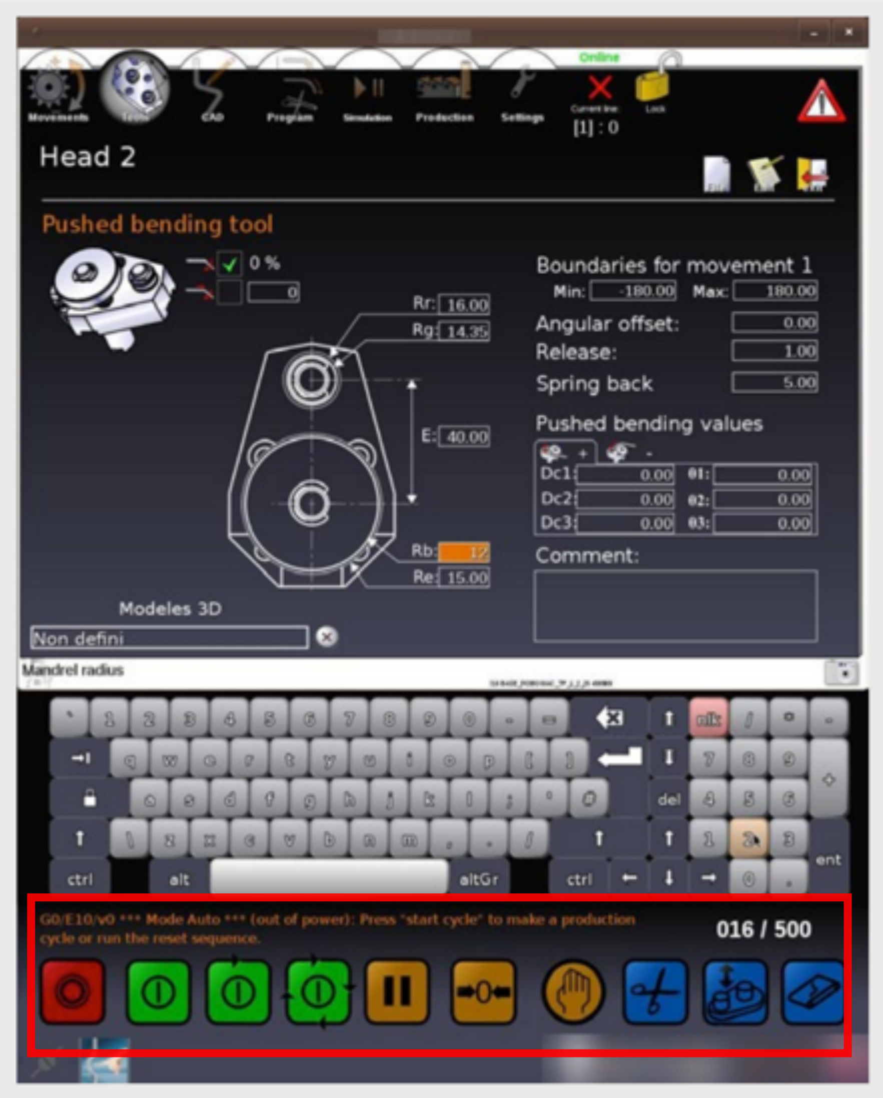
The issue can be more serious in the era of industry 4.0

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



Threats and Risks to exposed OT systems

Exposed ICSs



[1] : 0

Head 2

Pushed bending tool

☑ 0 %
□ 0

Rr: 16.00
Rg: 14.35
E: 40.00
Rb: 12
Re: 15.00

Boundaries for movement 1
Min: -180.00 Max: 180.00
Angular offset: 0.00
Release: 1.00
Spring back 5.00

Pushed bending values

Dc1:	0.00	θ1:	0.00
Dc2:	0.00	θ2:	0.00
Dc3:	0.00	θ3:	0.00

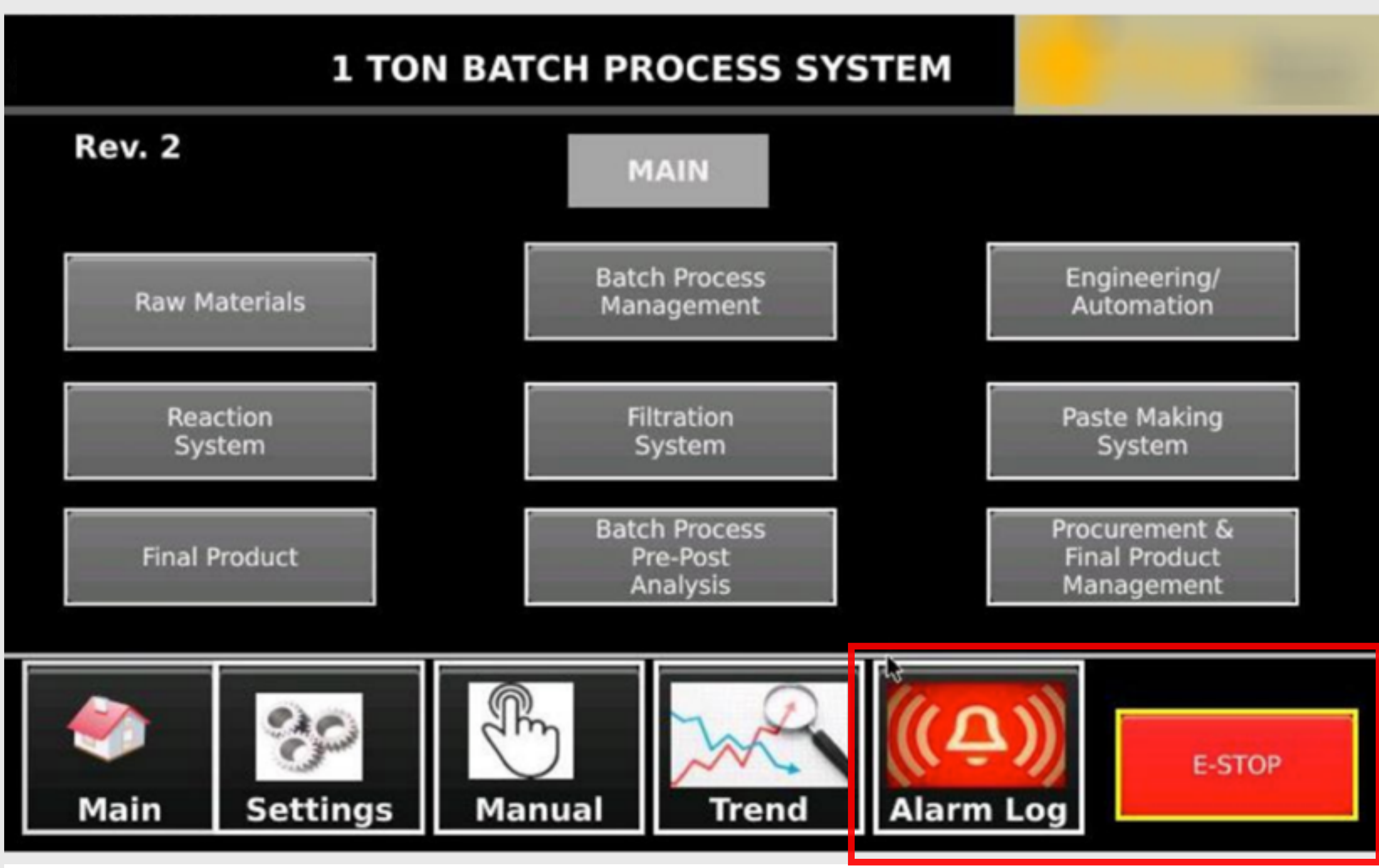
Comment:

Modeles 3D
Non defini

Mandrel radius

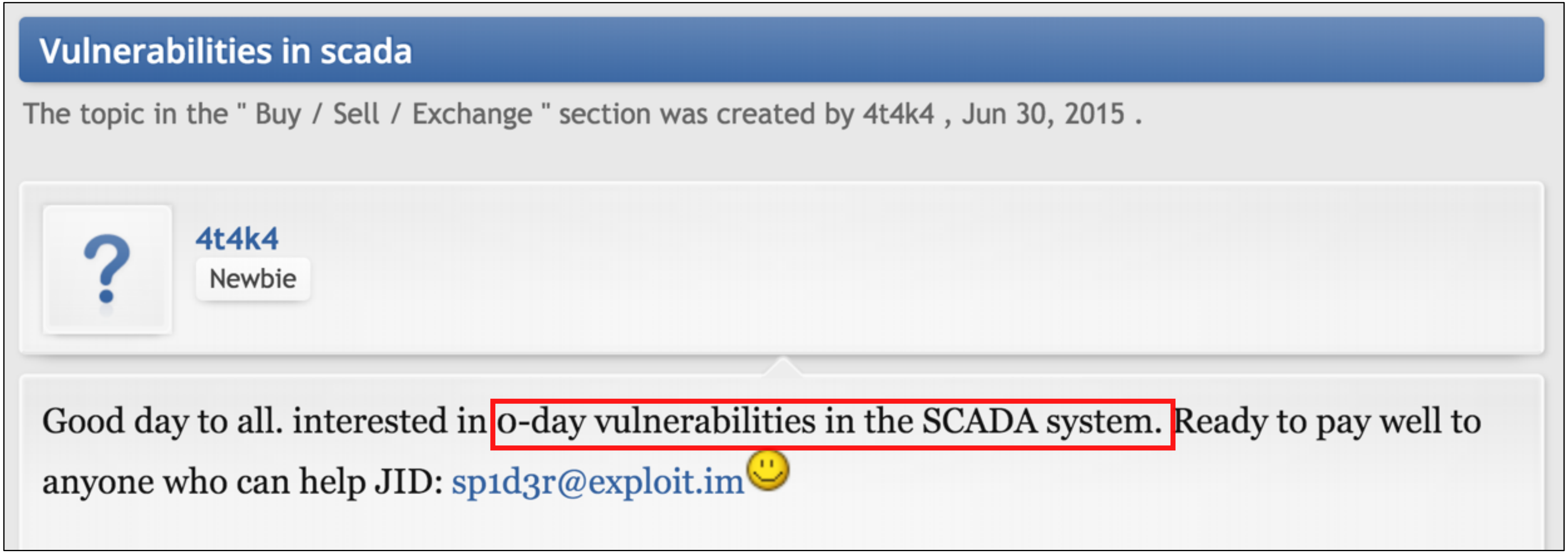
G0/E10/v0 *** Mode Auto *** (out of power): Press "start cycle" to make a production cycle or run the reset sequence.

016 / 500



Underground Activities related to Manufacturing industry

SCADA 0days dealt on the Underground



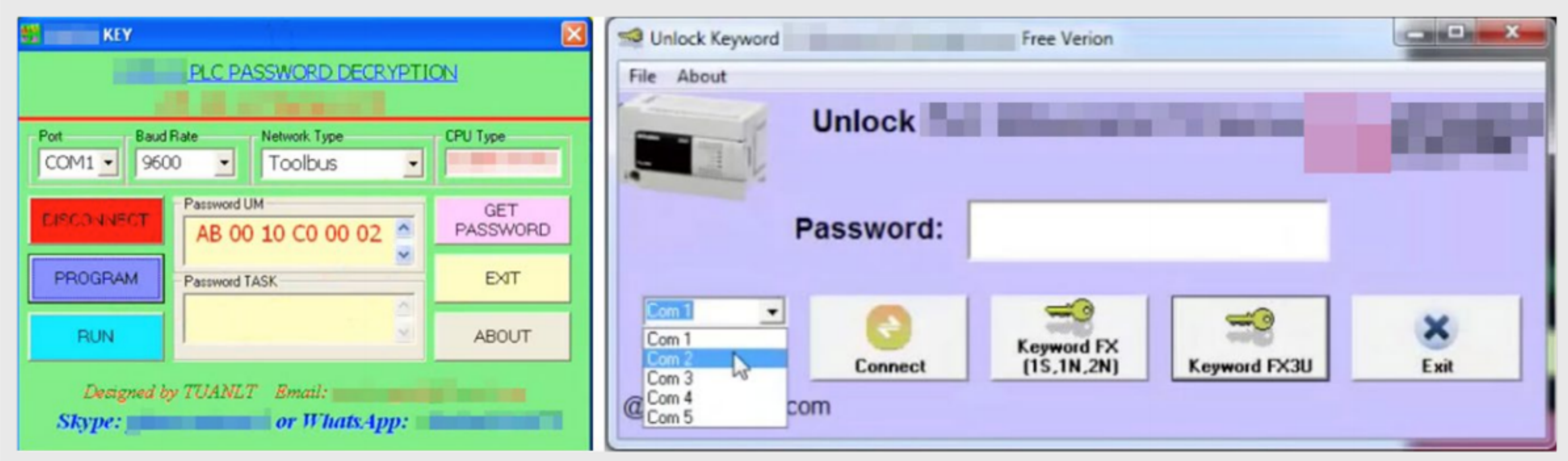
Vulnerabilities in scada

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



[redacted] KEY

PLC PASSWORD DECRYPTION

Port: COM1
Baud Rate: 9600
Network Type: Toolbus
CPU Type: [redacted]

Password UM: AB 00 10 C0 00 02

Password TASK:

Designed by TUANLT Email: [redacted]

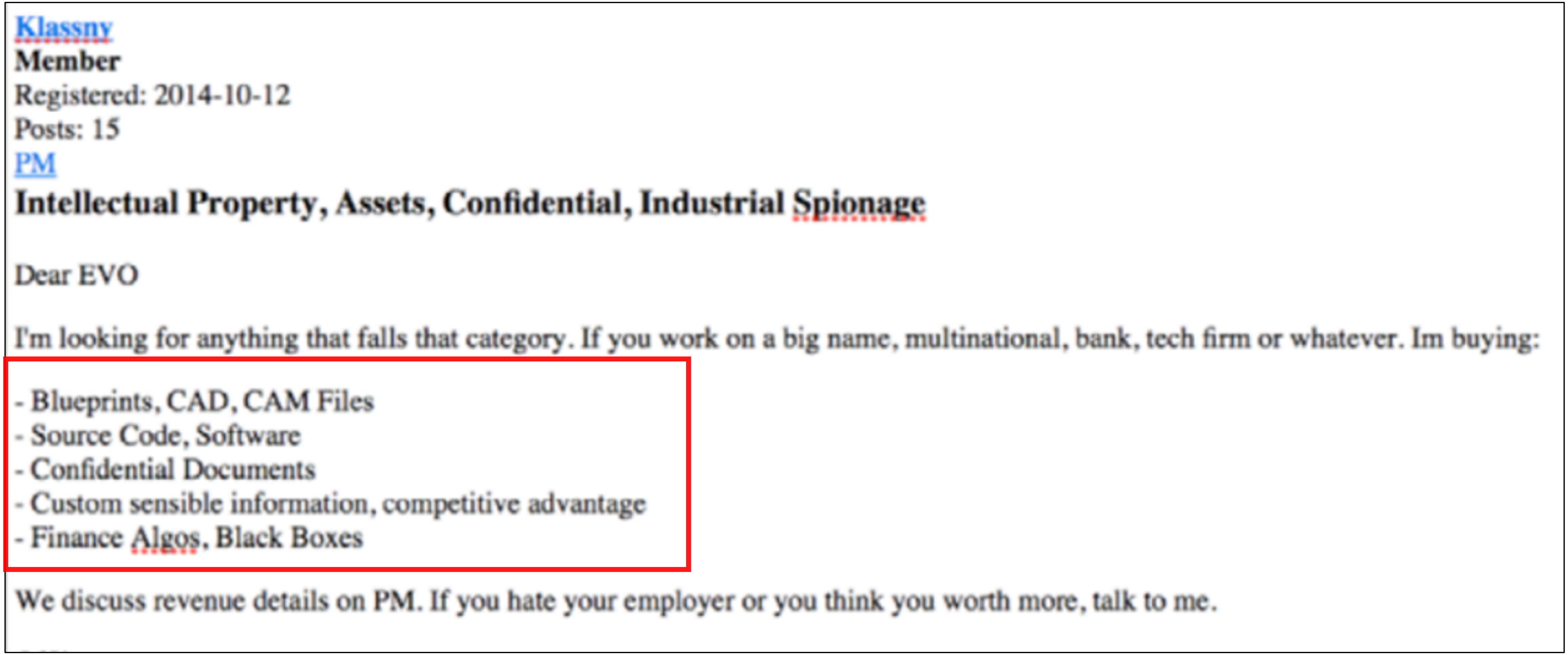
Skype: [redacted] *or WhatsApp:* [redacted]

Unlock Keyword [redacted] Free Verion

Unlock [redacted]

Password:

Com 1



Klassny
Member
Registered: 2014-10-12
Posts: 15
PM

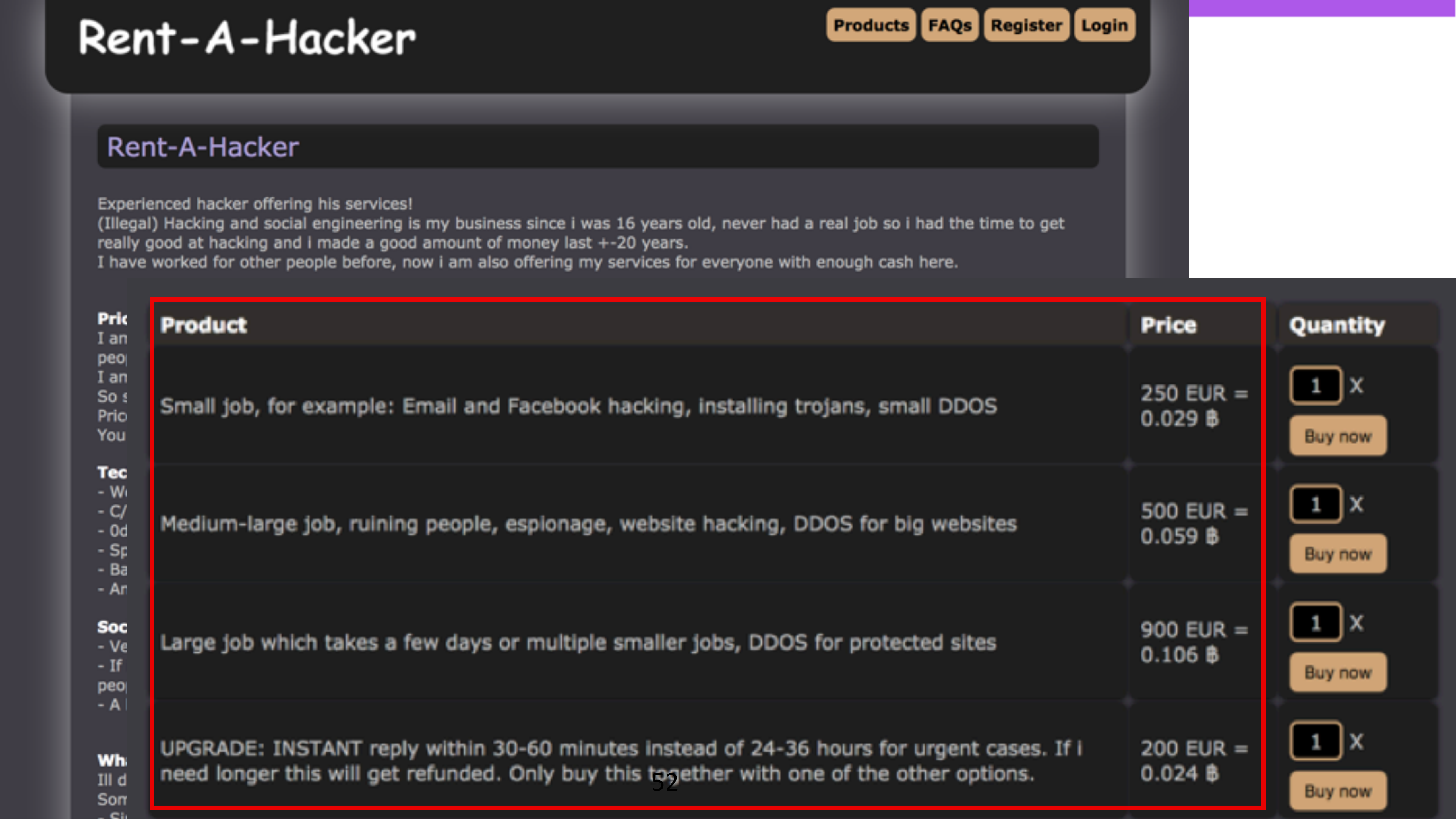
Intellectual Property, Assets, Confidential, Industrial Spionage

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.

Pric
I am
peo
I am
So s
Pric
You

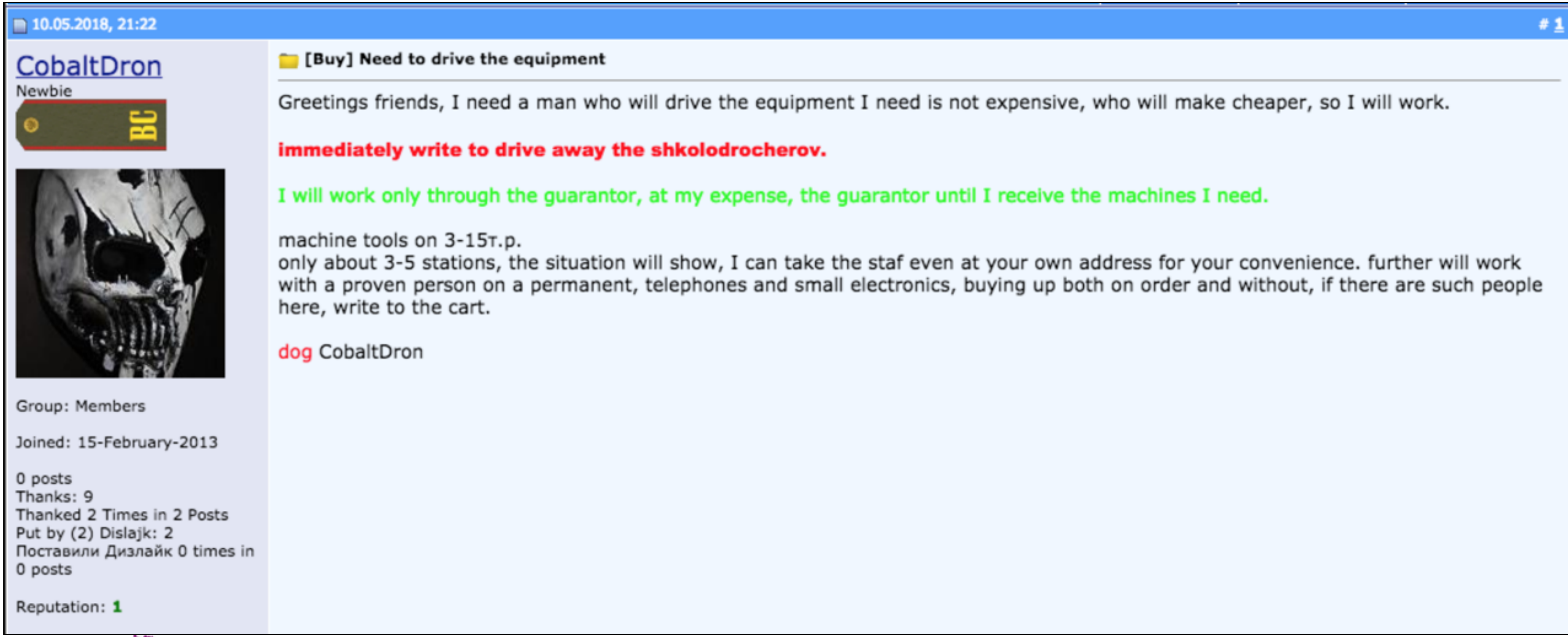
Tec
- W
- C/
- 0d
- Sp
- Ba
- An

Soc
- Ve
- If
peo
- A

Wh
Ill d
Som

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.029 ฿	1 X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.059 ฿	1 X Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites	900 EUR = 0.106 ฿	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 ฿	1 X Buy now

Industrial equipment purchase request



10.05.2018, 21:22 # 1

CobaltDron
Newbie

Group: Members

Joined: 15-February-2013

0 posts
Thanks: 9
Thanked 2 Times in 2 Posts
Put by (2) Dislajk: 2
Поставили Дизлайк 0 times in 0 posts

Reputation: 1

[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.

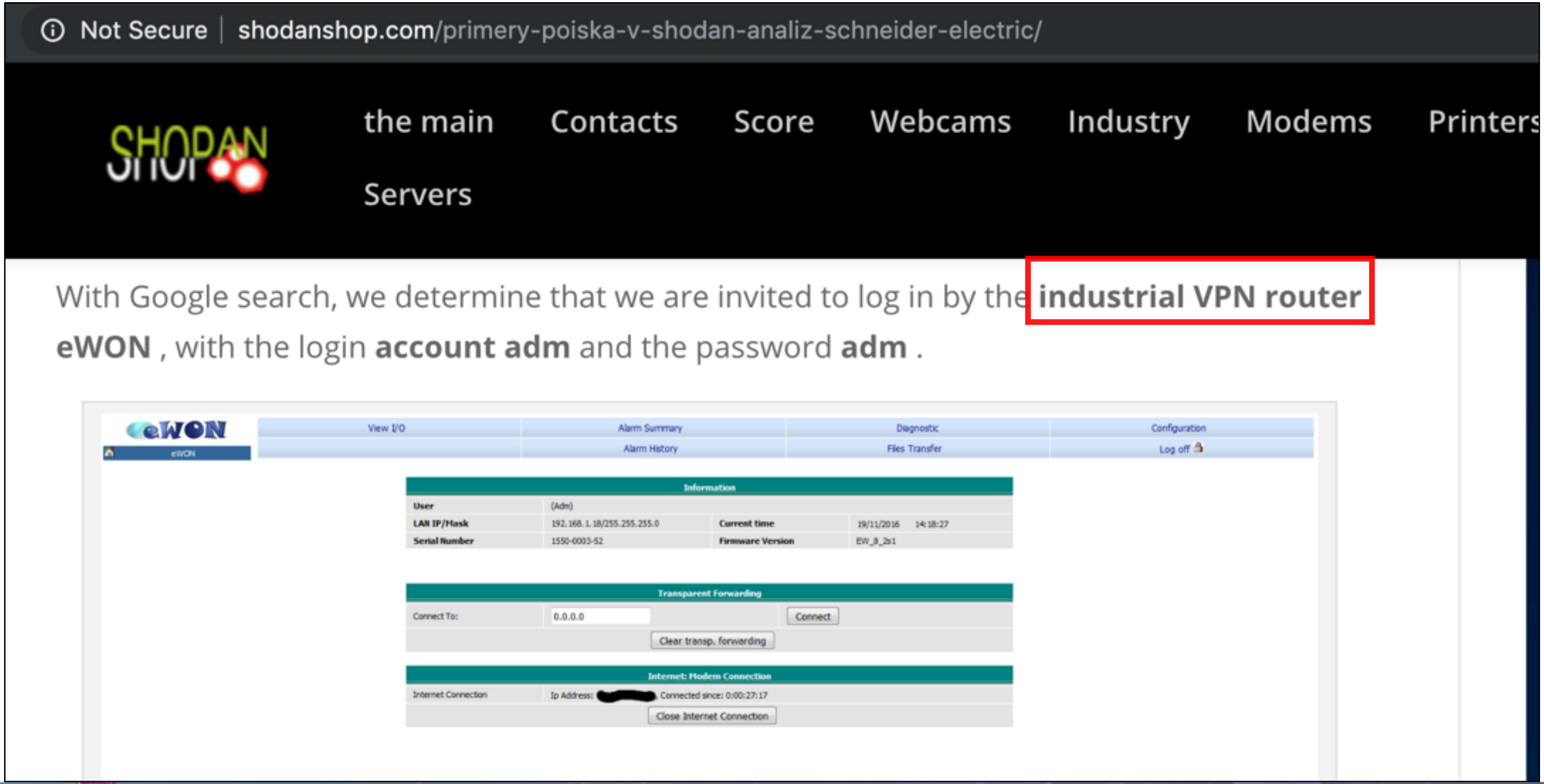
immediately write to drive away the shkolodrocherov.

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 staf 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 **industrial VPN router** **eWON** , with the login **account adm** and the password **adm** .

Information			
User	(Adm)		
LAN IP/Mask	192.168.1.18/255.255.255.0	**Current time**	19/11/2016 14:18:27
Serial Number	1550-0003-52	**Firmware Version**	EW_8_2s1

Transparent Forwarding

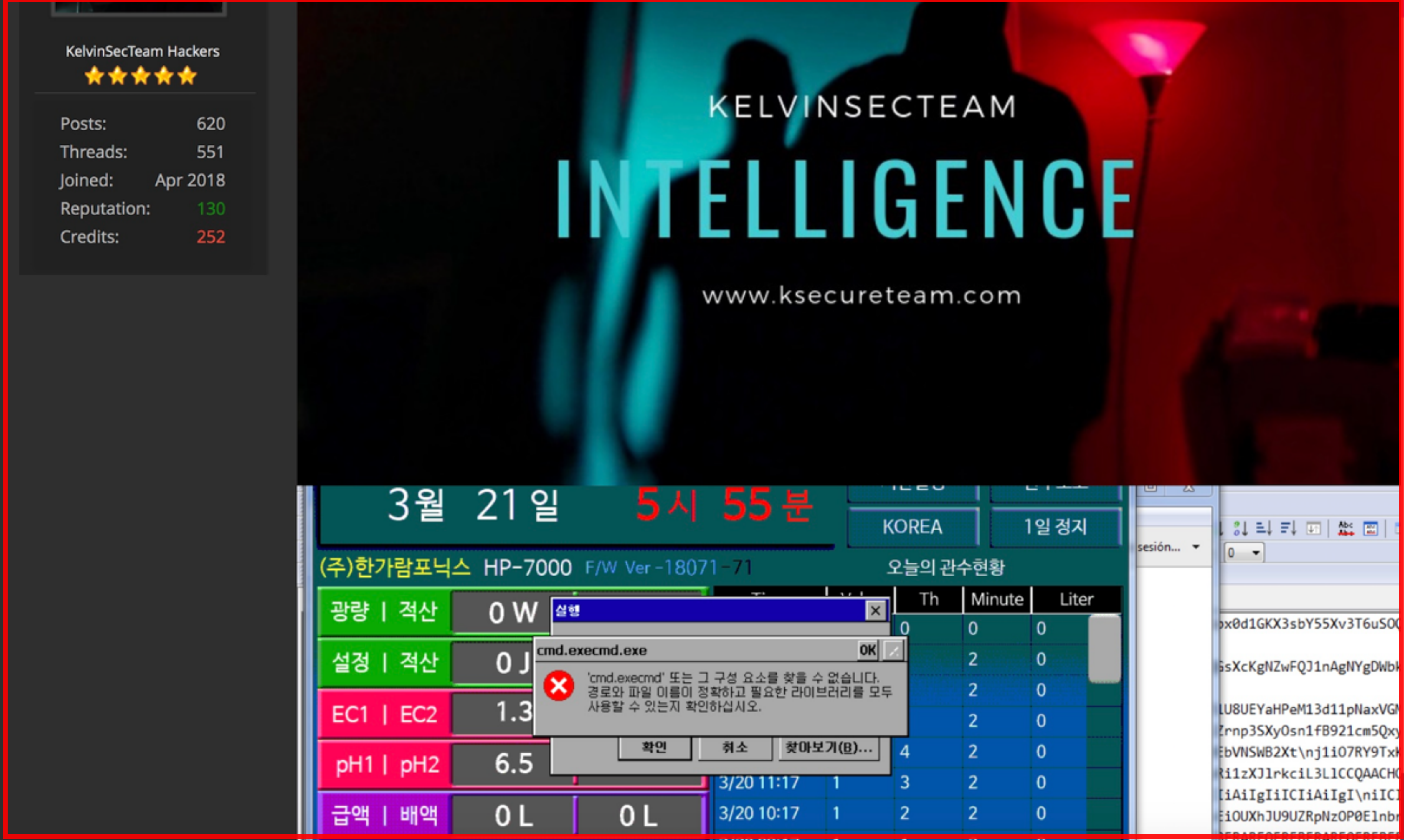
Connect To: 0.0.0.0 Connect

Clear transp. forwarding

Internet: Modem Connection

Internet Connection Ip Address: [redacted], Connected since: 0:00:27:17

Close Internet Connection



KelvinSecTeam Hackers

★★★★★

Posts: 620

Threads: 551

Joined: Apr 2018

Reputation: 130

Credits: 252

cmd.execmd.exe

'cmd.execmd' 또는 그 구성 요소를 찾을 수 없습니다. 경로와 파일 이름이 정확하고 필요한 라이브러리를 모두 사용할 수 있는지 확인하십시오.

OK

		Th	Minute	Liter
		0	0	0
			2	0
			2	0
			2	0
		4	2	0
3/20 11:17	1	3	2	0
3/20 10:17	1	2	2	0
3/20 09:17	1	1	2	0

px0d1GKX3sbY55Xv3T6uSO
GsXcKgNZwFQJ1nAgNYgDWb
LU8UEYaHPeM13d11pNaxVG
Zrnp3SXyOsn1fB921cm5Qx
EbVNSWB2Xt\nj1iO7RY9Tx
Ri1zXJlrkciL3L1CCQAACH
IiAiIgIiICIiAiIgI\niIC
EiOUXhJU9UZRpNzOP0E1nb

Conclusion and Final Remarks

Impacts on the Manufacturing Industry

- Productivity Impact Through Production Disruption
- Business Impact Through Market Disruption
- Reputational Risks

Securing your journey to Industry 4.0

- Manufacturing industry is in significant change
- Manufacturing companies need to be aware of the emerging threats and risks
- IT administrators need to cooperate with OT engineers

Thank you!

TREND MICRO | research

Bakuei_Matsukawa

Vladimir_Kropotov

Fyodor_Yarochkin

Ryan_Flores

<@trendmicro.com>

Trend Micro Research