txOne networks *The Leader of OT Zero Trust*

智慧製造環境中實際面臨的攻擊向量與務實有效的緩解策略

Mars Cheng, Canaan Kao

September 22, 2022

Mars Cheng and Canaan Kao

Mars Cheng

Manager, PSIRT and Threat Research at TXOne Networks

- Executive Director, Association of Hackers in Taiwan (HIT)
- ICS/SCADA, IoT, Malware Analysis and Enterprise Security
- Spoke at Black Hat, RSA Conference, DEF CON, HITCON, FIRST, SecTor, HITB, SINCON, ICS Cyber Security Conference USA and Asia, CYBERSEC, InfoSec Taiwan and so on
- Instructor of HITCON Training 2022/2021/2020/2019,CCoE Taiwan, Ministry of Education, Ministry of National Defense, Ministry of Economic Affairs in Taiwan, and Listed companies
- General Coordinator of HITCON (Hacks In Taiwan Conference) PEACE 2022 and 2021

Canaan Kao

Director, Threat Research at TXOne Networks

- Ph.D. in Communications Engineering, NTHU, ROC (Taiwan)
- A DPI/IDS/IPS engineer since 2001.
- Spoke at HITCON2014 CMT,HITCON2015 CMT and HITCON 2019.
- His primary research interests are in network security, intrusion detection systems, reversing engineering, malware detection, and ICS/embedded systems.

Outline

- ICS/SCADA Threats Overview
- The Practical Attack Vectors for Modern ICS/SCADA
- The Common Defense Strategies for Securing Read-World ICS Environment

txOne™ networks *The Leader of OT Zero Trust*

ICS/SCADA Threats Overview

關鍵基礎設施

- 影響國家經濟、公共衛生、環境或社會安全等設施
  - 公有 / 私有

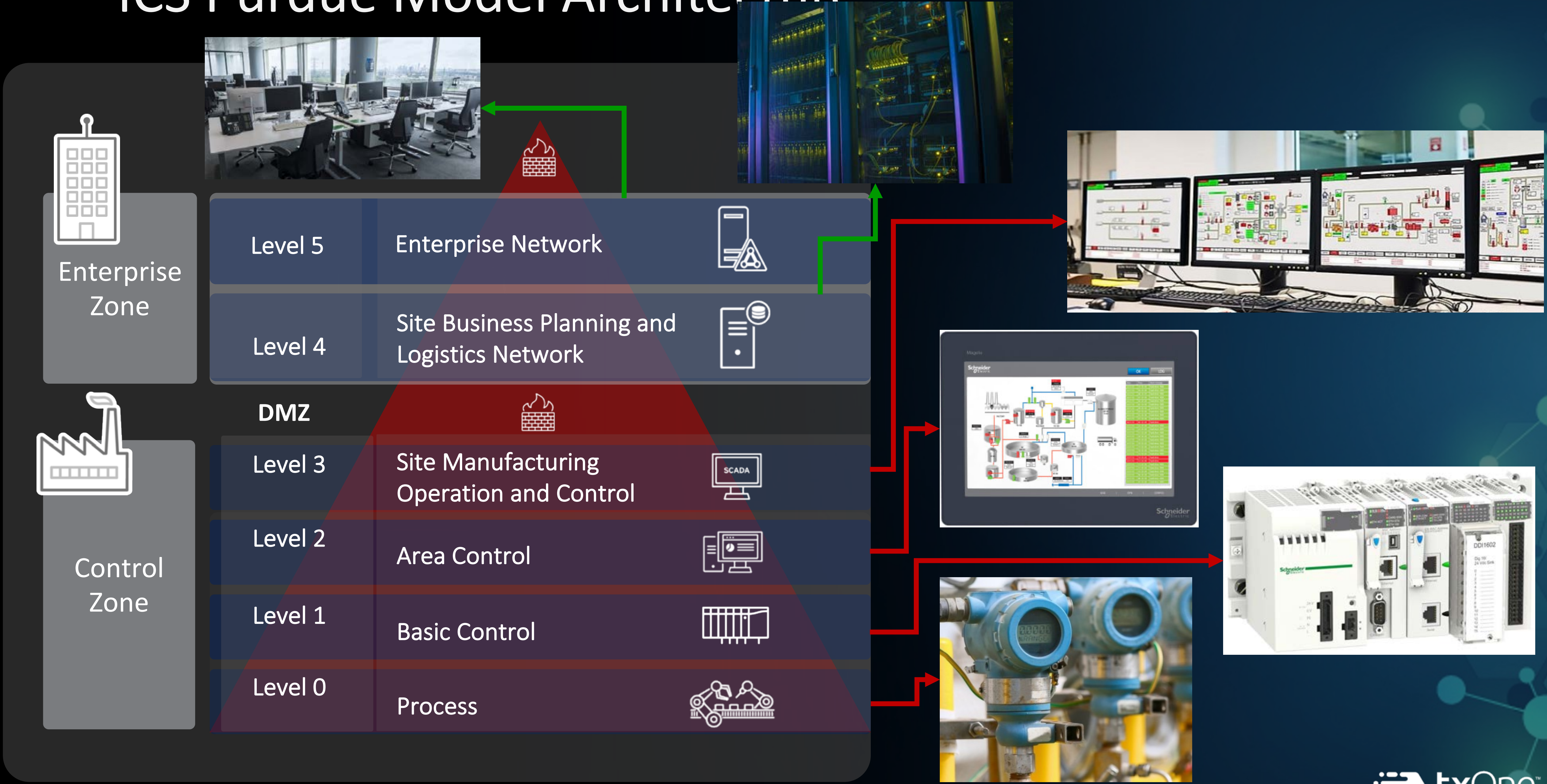
- 各國對關鍵基礎設施的定義稍有不同
  - 大多與能源、交通、通訊、政府、金融及醫療相關

能源　水資源　通訊傳播　交通

金融　緊急救援與醫院　政府機關　科學園區與工業區

能源	水資源	緊急救援與醫院	科學園區與工業區			金融	交通	通訊傳播	政府機關
台灣電力公司	台灣自來水	彰化基督教醫院	穩懋	億豐綜合工業	瑞昱半導體	上海商銀	台灣高鐵	中華電信	總統府
台灣中油		馬偕紀念醫院	中美矽晶製品	和碩聯合科技	和泰汽車	富邦金	長榮航空	台灣大哥大	行政院
台塑石化		長庚醫院	儒鴻企業	力成科技	大立光	華南金	中華航空	遠傳電信	立法院
欣欣天然氣		高雄榮民總醫院	裕隆日產汽車	緯穎科技服務	聯詠科技	國泰世華商業銀行	長榮海運		司法院
新海瓦斯		高雄醫學大學附設醫院	聯強國際	光寶科技	台灣水泥	永豐金	萬海航運		考試院
大台北區瓦斯		三軍總醫院	健鼎科技	英業達	友達光電	元大金	陽明海運		監察院
		台中榮民總醫院	日月光半導體製造	仁寶電腦工業	上銀科技	中華開發金控	中央氣象局		台灣其他政府機關
		台北榮民總醫院	旭隼科技	群聯電子	台灣塑膠工業	台新金	臺灣鐵路管理局		
		台北市立萬芳醫院	巨大機械工業	廣達電腦	致茂電子	彰化商業銀行			
		奇美醫院	群創光電	欣興電子	南亞塑膠工業	中央銀行			
		中國醫藥大學附設醫院	亞德客	中租控股	豐泰企業	中華郵政			
		台灣大學附設醫院	國巨	寶成工業	美利達工業	臺灣中小企業銀行			
		花蓮慈濟醫院	聯華電子	正新橡膠工業	台灣積體電路製造	兆豐金			
		亞東紀念醫院	宏碁	智邦科技	東元電機	新光金			
		中山醫學大學附設醫院	緯創資通	大聯大投資控股	華邦電子	第一金			
		國泰綜合醫院	遠東新世紀	亞洲水泥	微星科技	金融監督管理委員會			
		成功大學附設醫院	研華科技	譜瑞科技	技嘉科技				
		新光吳火獅紀念醫院	合一生技	世界先進積體電路	鴻海/鴻準				
			華新科技	南亞科技	南亞電路板				
			華碩電腦	可成科技	統一企業				
			祥碩科技	富邦媒體科技	聯發科技				
			臻鼎科技	中國鋼鐵	旺宏電子				
			台灣化學纖維	台達電					

ICS Purdue Model Architecture



Enterprise Zone

Level 5 | Enterprise Network

Level 4 | Site Business Planning and Logistics Network

DMZ

Control Zone

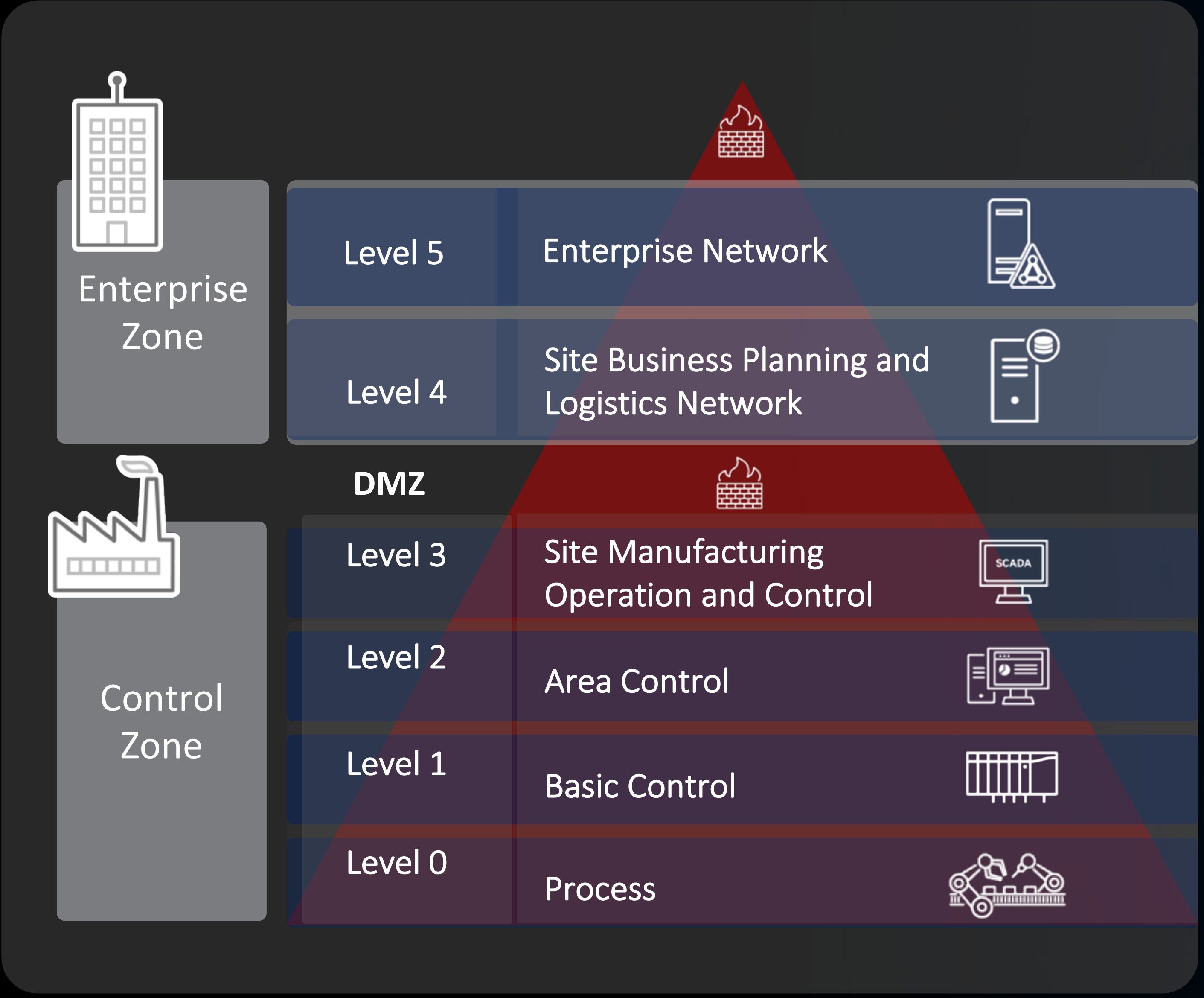
Level 3 | Site Manufacturing Operation and Control

Level 2 | Area Control

Level 1 | Basic Control

Level 0 | Process

ICS Purdue Model Architecture



Enterprise Zone

Level 5 Enterprise Network

Level 4 Site Business Planning and Logistics Network

DMZ

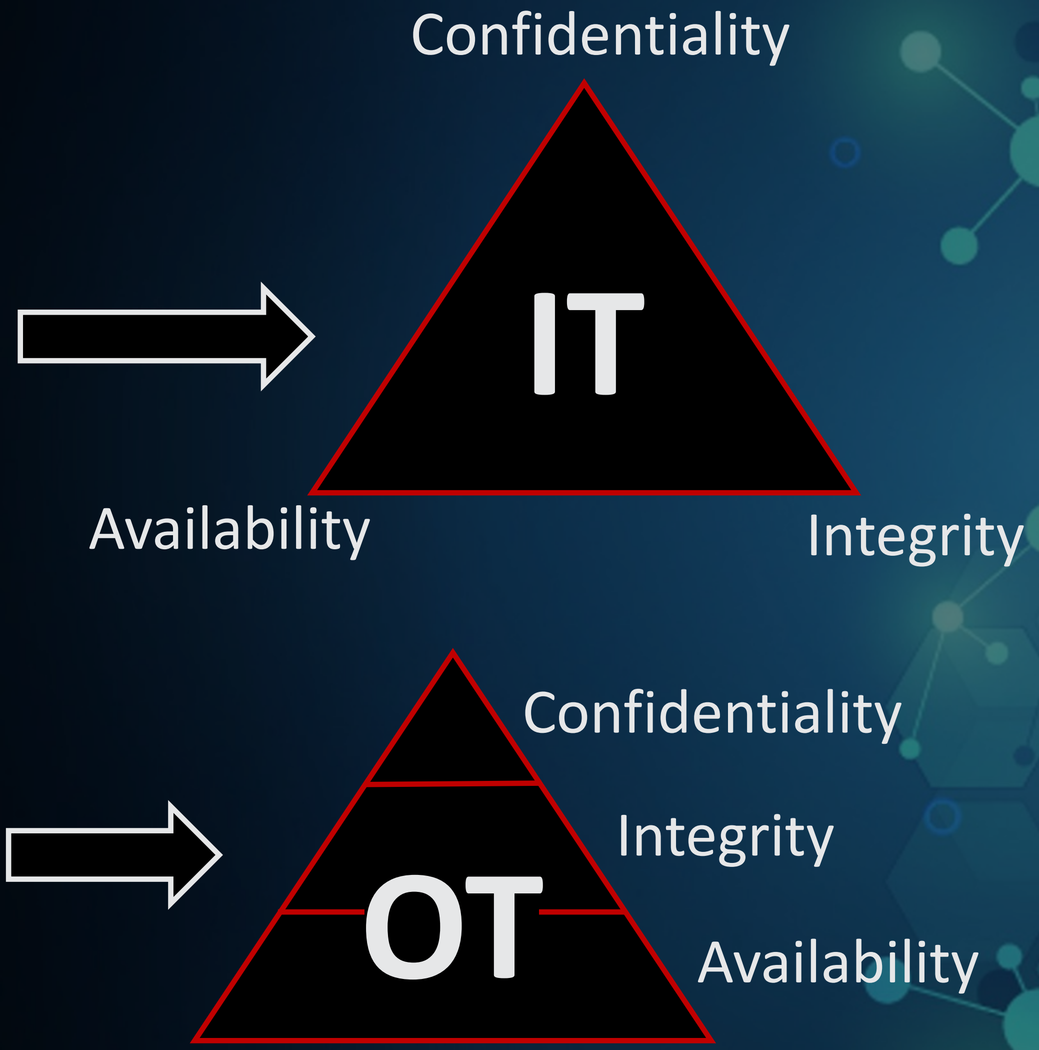
Control Zone

Level 3 Site Manufacturing Operation and Control

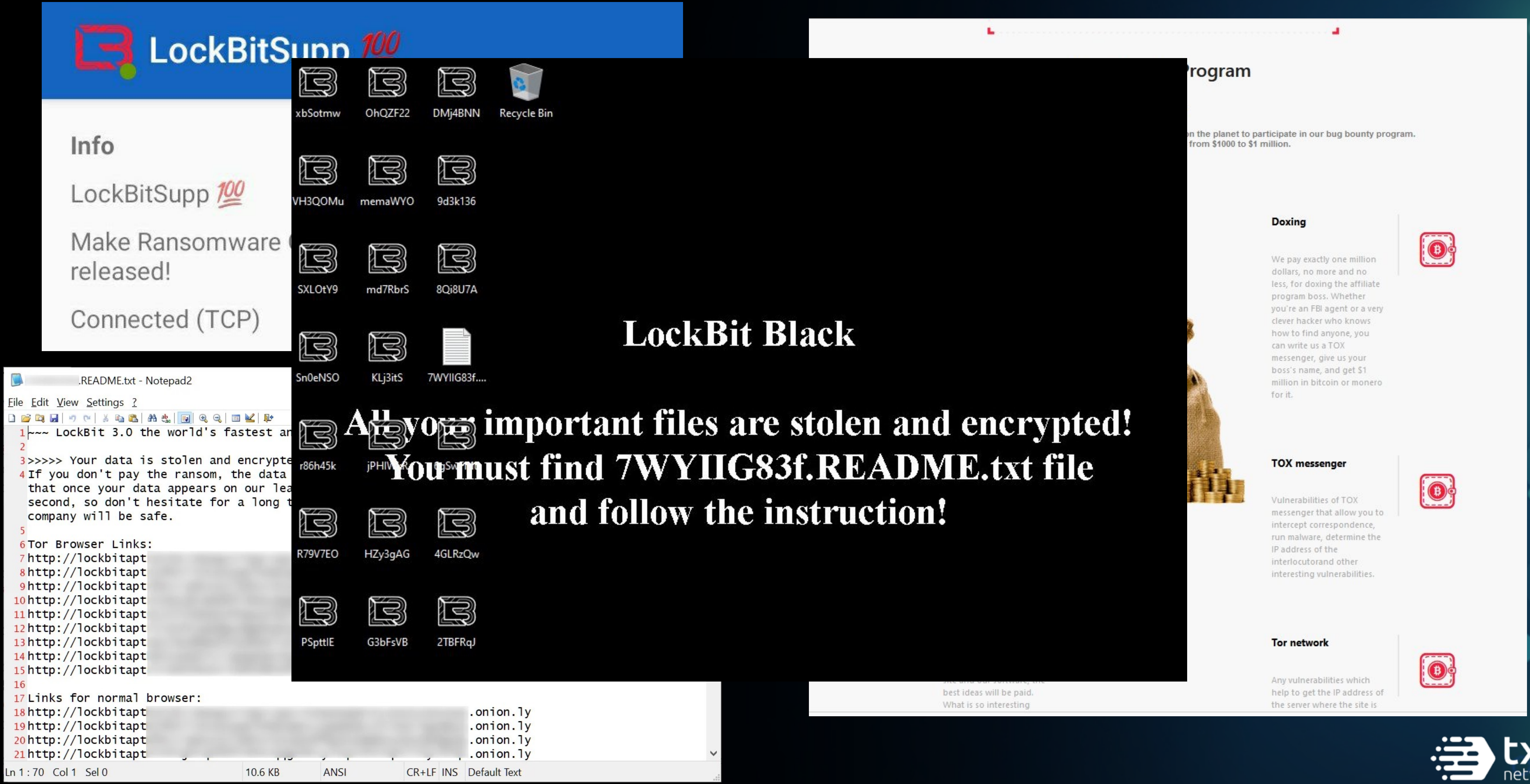
Level 2 Area Control

Level 1 Basic Control

Level 0 Process



2022.06 Lockbit 3.0 is officially released



LockBitSupp 💯

Info

LockBitSupp 💯

Make Ransomware
released!

Connected (TCP)

LockBit Black

All your important files are stolen and encrypted!
You must find 7WYIIG83f.README.txt file
and follow the instruction!

[redacted].README.txt - Notepad2

```
~~~ LockBit 3.0 the world's fastest ar

>>>>> Your data is stolen and encrypte
If you don't pay the ransom, the data
that once your data appears on our lea
second, so don't hesitate for a long t
company will be safe.

Tor Browser Links:
http://lockbitapt[redacted]
http://lockbitapt
http://lockbitapt
http://lockbitapt
http://lockbitapt
http://lockbitapt
http://lockbitapt
http://lockbitapt
http://lockbitapt

Links for normal browser:
http://lockbitapt[redacted].onion.ly
http://lockbitapt.onion.ly
http://lockbitapt.onion.ly
http://lockbitapt.onion.ly
```

Ln 1 : 70 Col 1 Sel 0 10.6 KB ANSI CR+LF INS Default Text

rogram

n the planet to participate in our bug bounty program.
from $1000 to $1 million.

Doxing

We pay exactly one million dollars, no more and no less, for doxing the affiliate program boss. Whether you're an FBI agent or a very clever hacker who knows how to find anyone, you can write us a TOX messenger, give us your boss's name, and get $1 million in bitcoin or monero for it.

TOX messenger

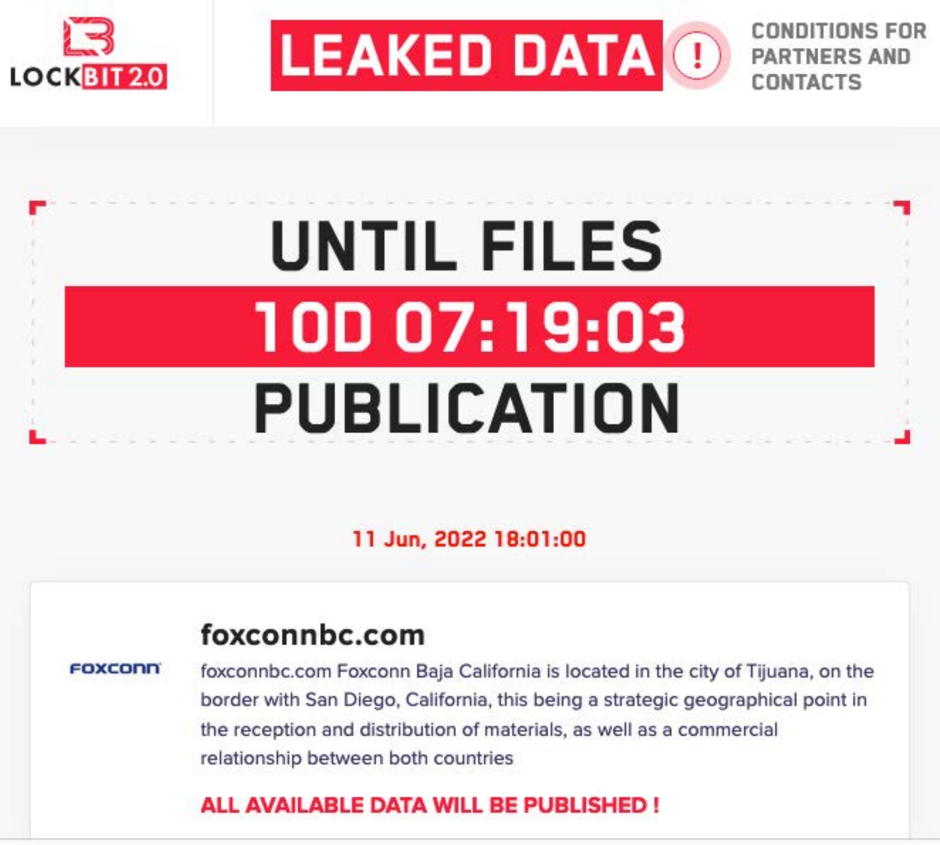
Vulnerabilities of TOX messenger that allow you to intercept correspondence, run malware, determine the IP address of the interlocutorand other interesting vulnerabilities.

Tor network

Any vulnerabilities which help to get the IP address of the server where the site is

best ideas will be paid.
What is so interesting

2022.06 Foxconn Confirms Ransomware Hit Factory in Mexico by LockBit 2.0



LEAKED DATA !

CONDITIONS FOR PARTNERS AND CONTACTS

UNTIL FILES

10D 07:19:03

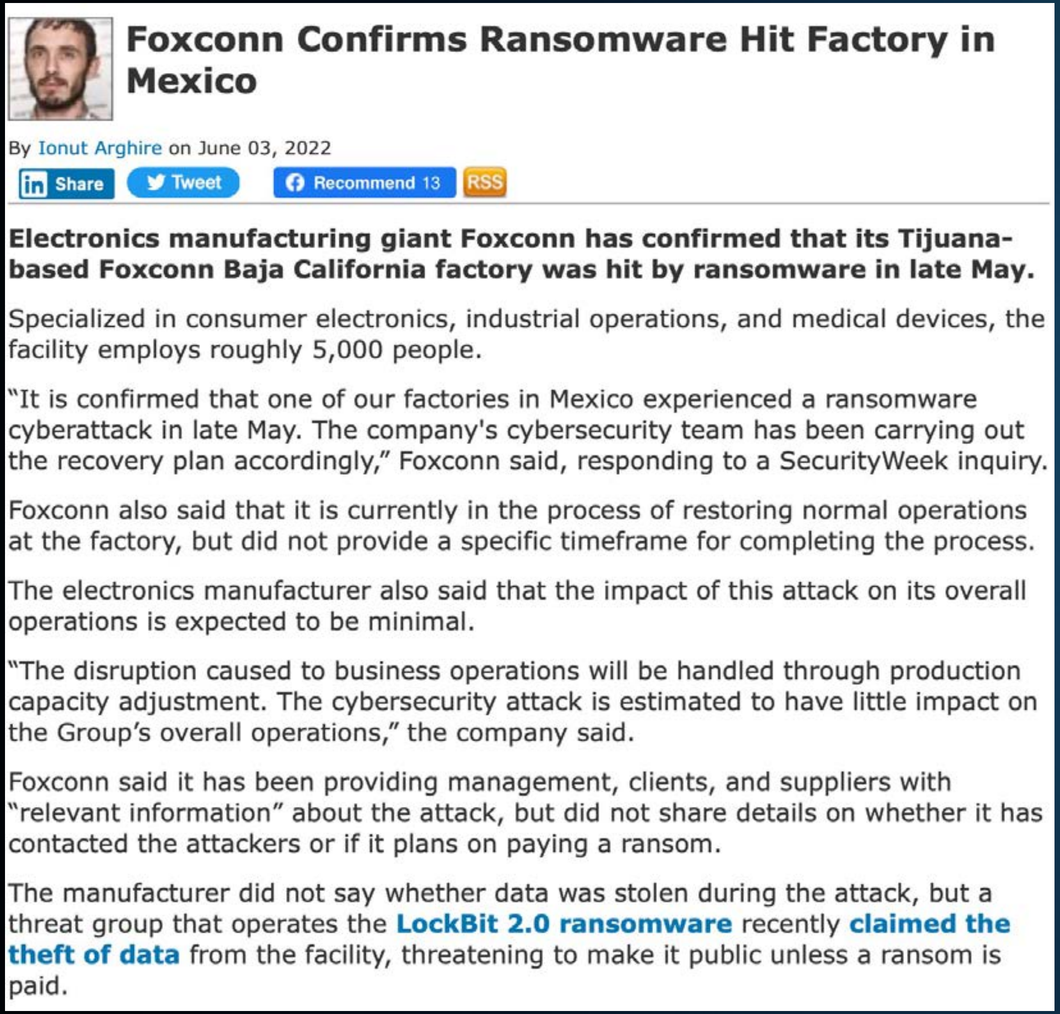
PUBLICATION

11 Jun, 2022 18:01:00

foxconnbc.com

foxconnbc.com Foxconn Baja California is located in the city of Tijuana, on the border with San Diego, California, this being a strategic geographical point in the reception and distribution of materials, as well as a commercial relationship between both countries

ALL AVAILABLE DATA WILL BE PUBLISHED !



Foxconn Confirms Ransomware Hit Factory in Mexico

By Ionut Arghire on June 03, 2022

Electronics manufacturing giant Foxconn has confirmed that its Tijuana-based Foxconn Baja California factory was hit by ransomware in late May.

Specialized in consumer electronics, industrial operations, and medical devices, the facility employs roughly 5,000 people.

"It is confirmed that one of our factories in Mexico experienced a ransomware cyberattack in late May. The company's cybersecurity team has been carrying out the recovery plan accordingly," Foxconn said, responding to a SecurityWeek inquiry.

Foxconn also said that it is currently in the process of restoring normal operations at the factory, but did not provide a specific timeframe for completing the process.

The electronics manufacturer also said that the impact of this attack on its overall operations is expected to be minimal.

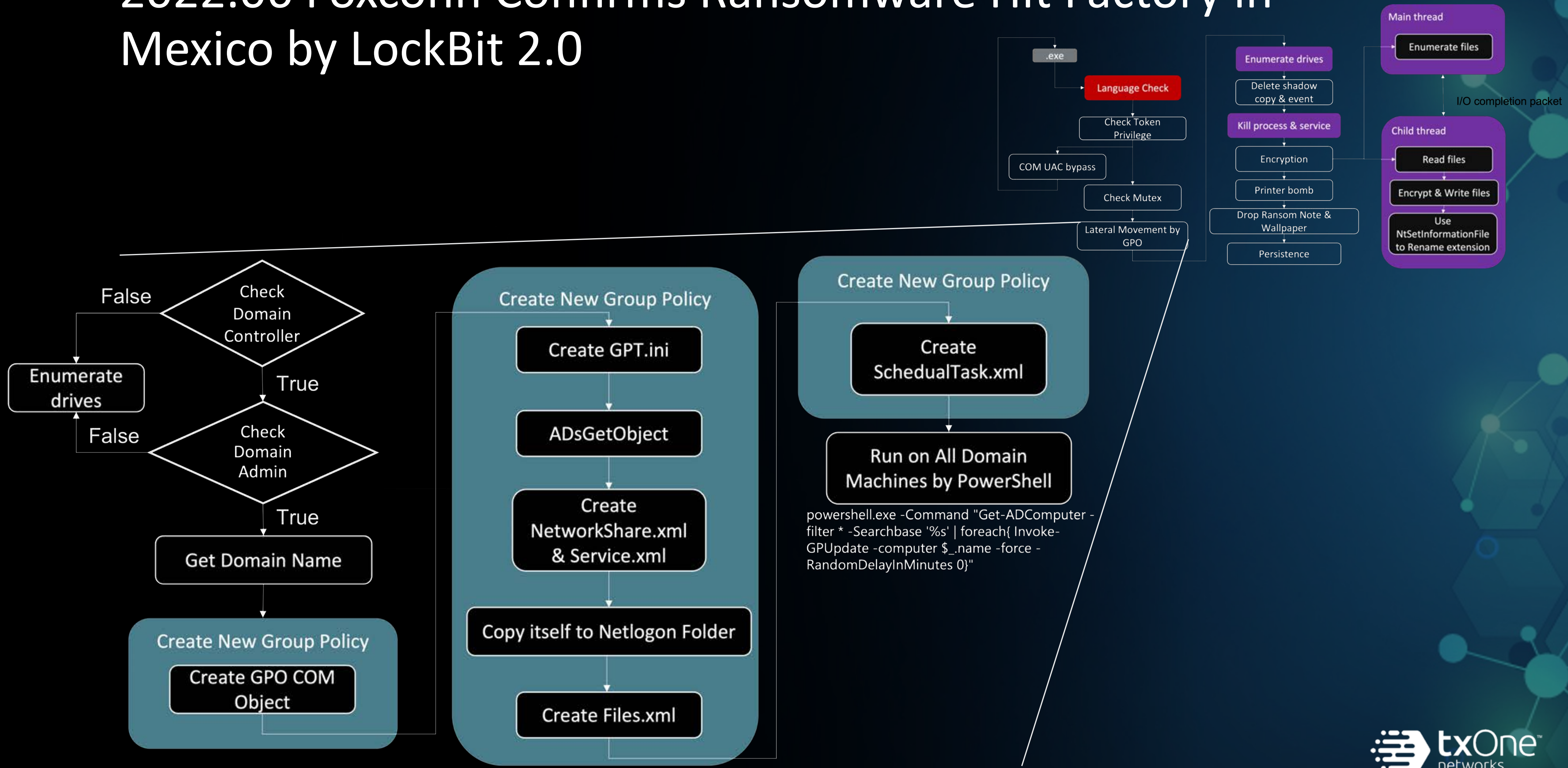
"The disruption caused to business operations will be handled through production capacity adjustment. The cybersecurity attack is estimated to have little impact on the Group's overall operations," the company said.

Foxconn said it has been providing management, clients, and suppliers with "relevant information" about the attack, but did not share details on whether it has contacted the attackers or if it plans on paying a ransom.

The manufacturer did not say whether data was stolen during the attack, but a threat group that operates the **LockBit 2.0 ransomware** recently **claimed the theft of data** from the facility, threatening to make it public unless a ransom is paid.

https://www.securityweek.com/foxconn-confirms-ransomware-hit-factory-mexico

2022.06 Foxconn Confirms Ransomware Hit Factory in Mexico by LockBit 2.0



```
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"
```

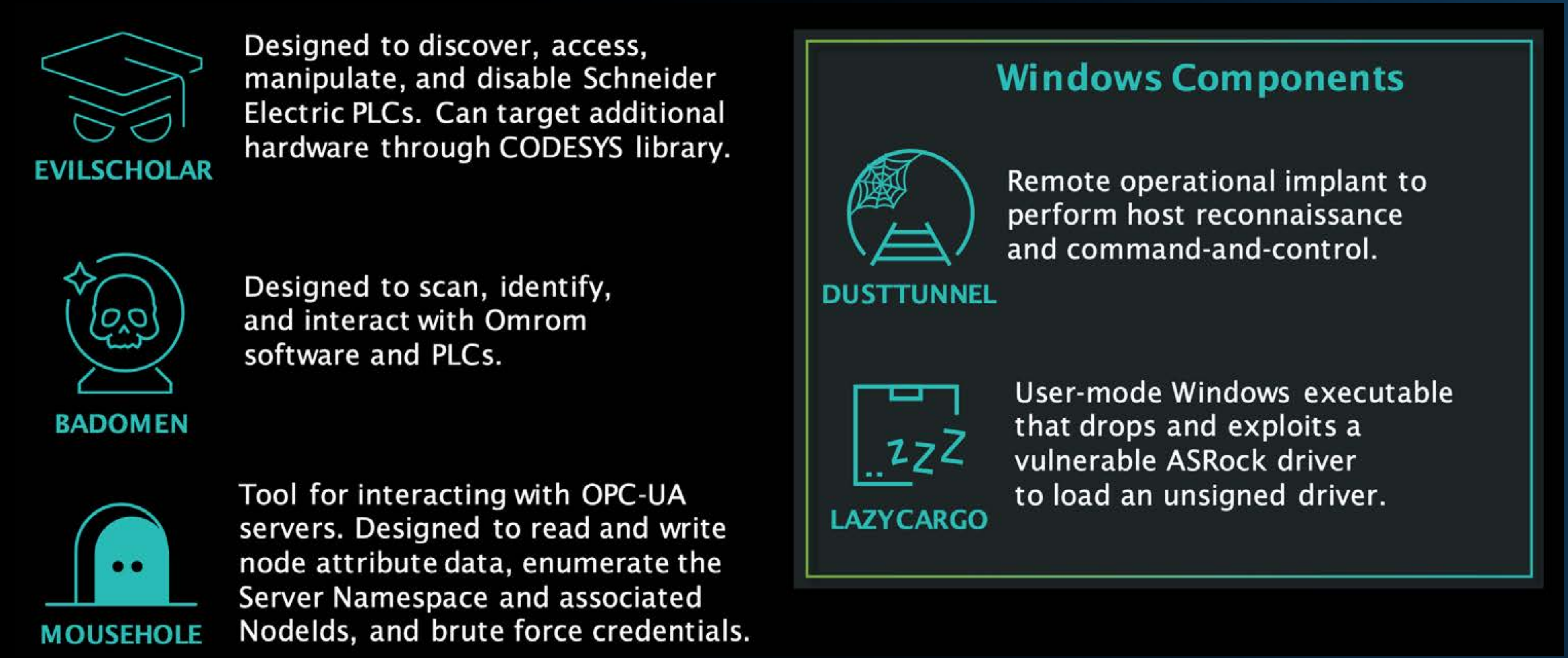
2022.04 PIPEDREAM Malware Targeting Industrial Control Systems (ICS)

- CHERNOVITE
  - Discovered in early 2022 by a partner
  - Partner shared the insights with Dragos to help identify/analyze the malware PIPEDREAM
  - CHERNOVITE is a threat group that has not yet employed their capability, PIPEDREAM, for its intended (disruptive/destructive) effects – their assessed intent is disruptive in nature
  - CHERNOVITE's initial target set appears to be U.S. Liquid Natural Gas and key Electric Power sites
  - CHERNOVITE's capability is in no way limited to those industries and is the most flexible ICS attack framework to date

https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/

2022.04 PIPEDREAM Malware Targeting Industrial Control Systems (ICS)

- PIPEDREAM Components



EVILSCHOLAR

Designed to discover, access, manipulate, and disable Schneider Electric PLCs. Can target additional hardware through CODESYS library.

BADOMEN

Designed to scan, identify, and interact with Omrom software and PLCs.

MOUSEHOLE

Tool for interacting with OPC-UA servers. Designed to read and write node attribute data, enumerate the Server Namespace and associated NodeIds, and brute force credentials.

Windows Components

DUSTTUNNEL

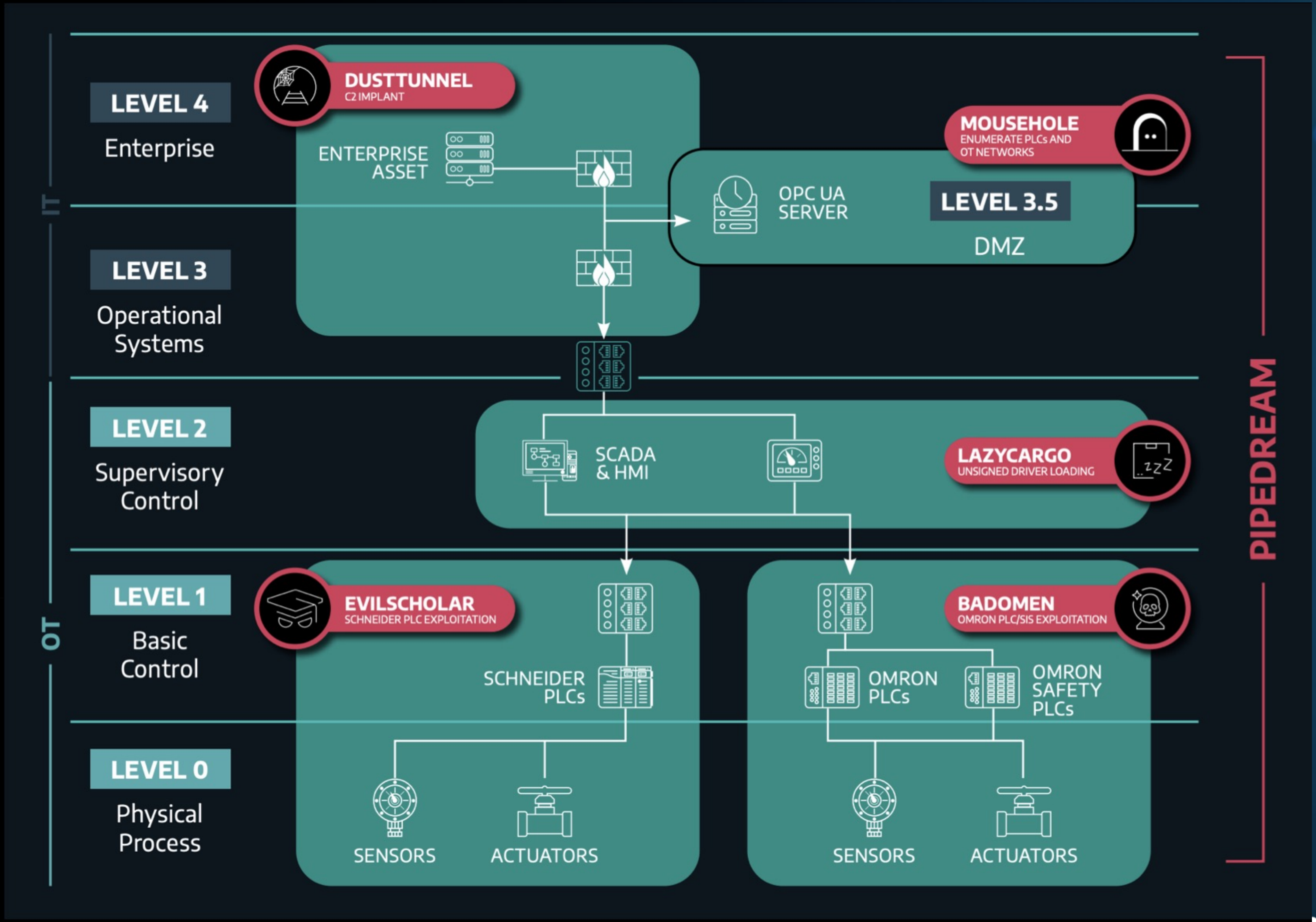
Remote operational implant to perform host reconnaissance and command-and-control.

LAZYCARGO

User-mode Windows executable that drops and exploits a vulnerable ASRock driver to load an unsigned driver.

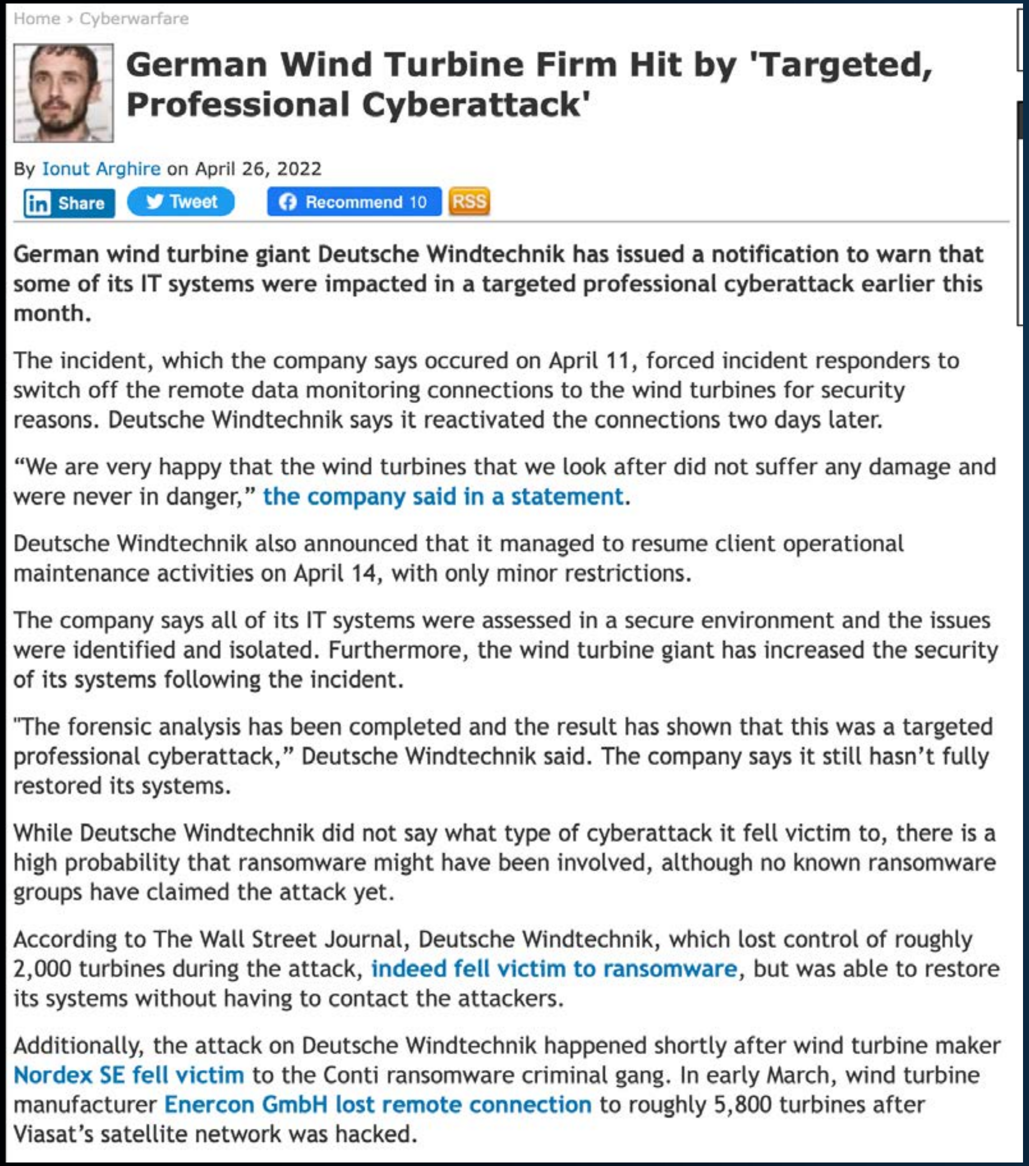
https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/

2022.04 PIPEDREAM Malware Targeting Industrial Control Systems (ICS)



txOne networks

2022.04 German Wind Turbine Firm Hit by Targeted and Professional Cyberattack



German Wind Turbine Firm Hit by 'Targeted, Professional Cyberattack'

By Ionut Arghire on April 26, 2022

German wind turbine giant Deutsche Windtechnik has issued a notification to warn that some of its IT systems were impacted in a targeted professional cyberattack earlier this month.

The incident, which the company says occured on April 11, forced incident responders to switch off the remote data monitoring connections to the wind turbines for security reasons. Deutsche Windtechnik says it reactivated the connections two days later.

“We are very happy that the wind turbines that we look after did not suffer any damage and were never in danger,” the company said in a statement.

Deutsche Windtechnik also announced that it managed to resume client operational maintenance activities on April 14, with only minor restrictions.

The company says all of its IT systems were assessed in a secure environment and the issues were identified and isolated. Furthermore, the wind turbine giant has increased the security of its systems following the incident.

"The forensic analysis has been completed and the result has shown that this was a targeted professional cyberattack,” Deutsche Windtechnik said. The company says it still hasn’t fully restored its systems.

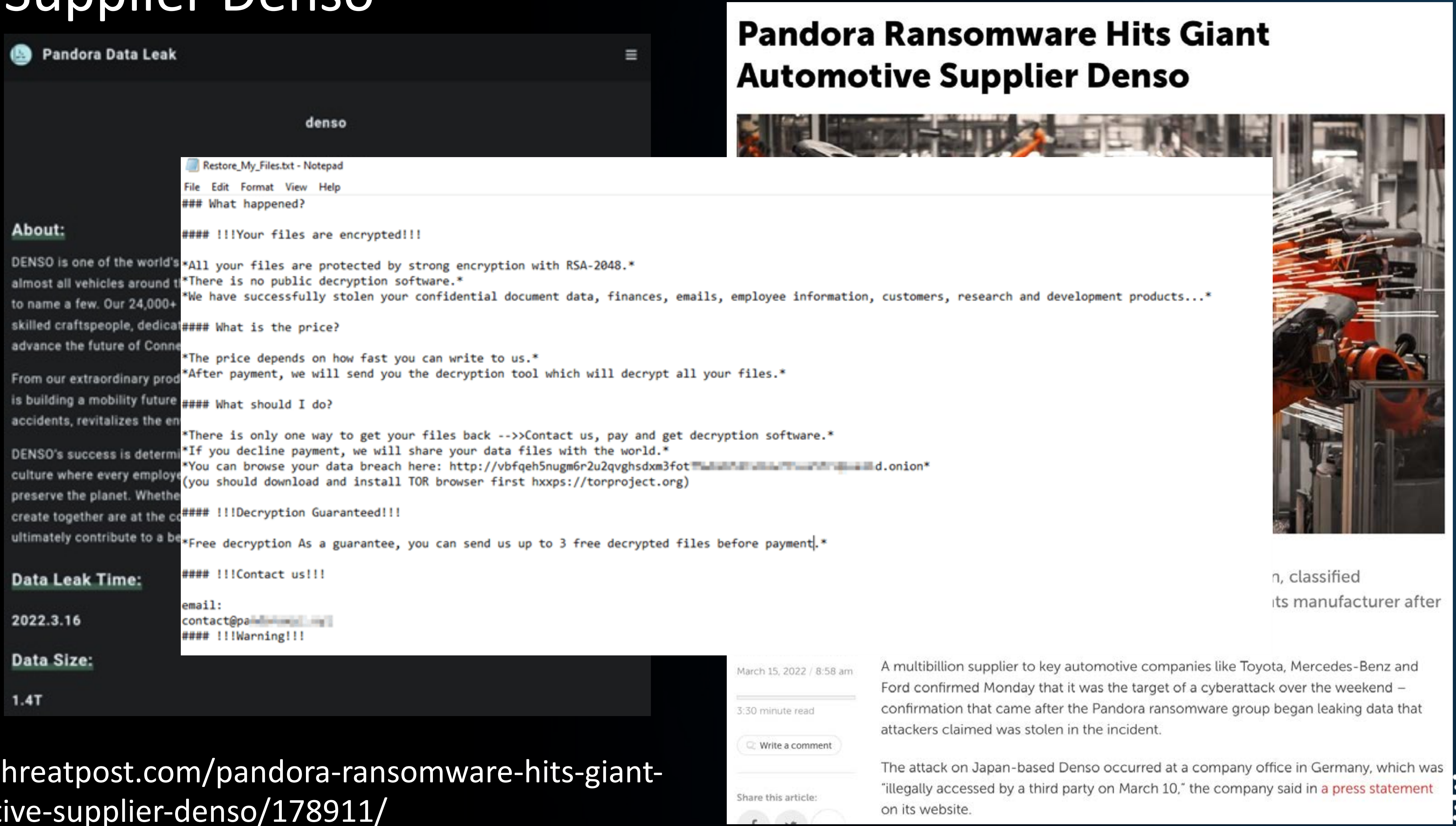
While Deutsche Windtechnik did not say what type of cyberattack it fell victim to, there is a high probability that ransomware might have been involved, although no known ransomware groups have claimed the attack yet.

According to The Wall Street Journal, Deutsche Windtechnik, which lost control of roughly 2,000 turbines during the attack, indeed fell victim to ransomware, but was able to restore its systems without having to contact the attackers.

Additionally, the attack on Deutsche Windtechnik happened shortly after wind turbine maker Nordex SE fell victim to the Conti ransomware criminal gang. In early March, wind turbine manufacturer Enercon GmbH lost remote connection to roughly 5,800 turbines after Viasat’s satellite network was hacked.

https://www.securityweek.com/german-wind-turbine-firm-discloses-targeted-professional-cyberattack

2022.03 Pandora Ransomware Hits Giant Automotive Supplier Denso



denso

About:

DENSO is one of the world's
almost all vehicles around t
to name a few. Our 24,000+
skilled craftspeople, dedicat
advance the future of Conne

From our extraordinary prod
is building a mobility future
accidents, revitalizes the en

DENSO's success is determi
culture where every employe
preserve the planet. Whethe
create together are at the c
ultimately contribute to a be

Data Leak Time:

2022.3.16

Data Size:

1.4T

```
### What happened?

#### !!!Your files are encrypted!!!

*All your files are protected by strong encryption with RSA-2048.*
*There is no public decryption software.*
*We have successfully stolen your confidential document data, finances, emails, employee information, customers, research and development products...*
#### What is the price?

*The price depends on how fast you can write to us.*
*After payment, we will send you the decryption tool which will decrypt all your files.*

#### What should I do?

*There is only one way to get your files back -->>Contact us, pay and get decryption software.*
*If you decline payment, we will share your data files with the world.*
*You can browse your data breach here: http://vbfqeh5nugm6r2u2qvghsdxm3fot[redacted]d.onion*
(you should download and install TOR browser first hxxps://torproject.org)

#### !!!Decryption Guaranteed!!!

*Free decryption As a guarantee, you can send us up to 3 free decrypted files before payment.*

#### !!!Contact us!!!

email:
contact@pa[redacted]
#### !!!Warning!!!
```

Pandora Ransomware Hits Giant Automotive Supplier Denso

n, classified
its manufacturer after

March 15, 2022 / 8:58 am

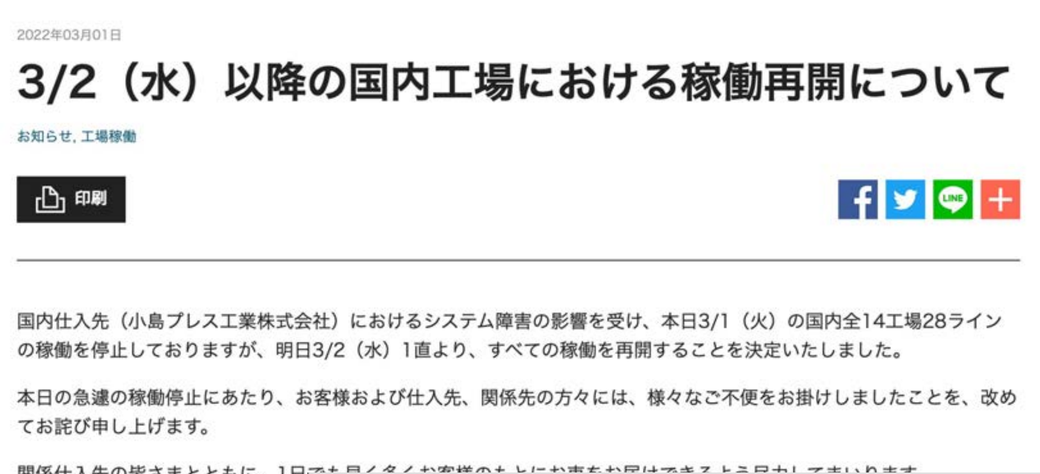
3:30 minute read

A multibillion supplier to key automotive companies like Toyota, Mercedes-Benz and Ford confirmed Monday that it was the target of a cyberattack over the weekend – confirmation that came after the Pandora ransomware group began leaking data that attackers claimed was stolen in the incident.

The attack on Japan-based Denso occurred at a company office in Germany, which was "illegally accessed by a third party on March 10," the company said in a press statement on its website.

https://threatpost.com/pandora-ransomware-hits-giant-automotive-supplier-denso/178911/

2022.02 Toyota Supply Chain Attack



2022年03月01日

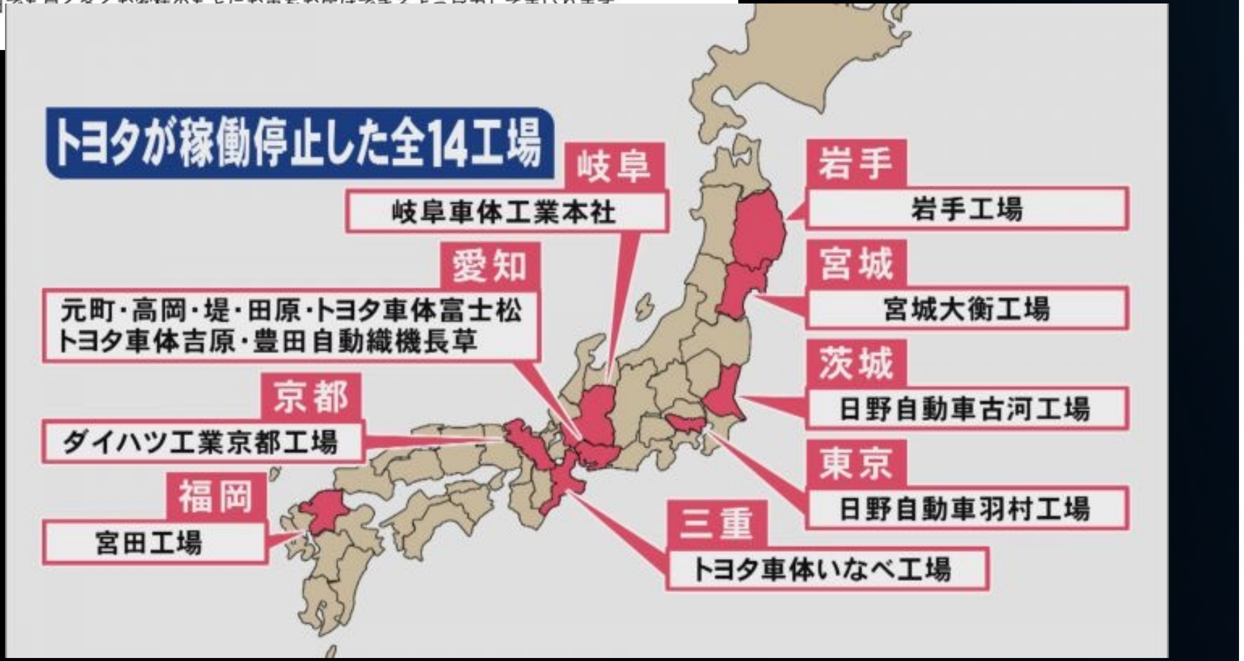
3/2（水）以降の国内工場における稼働再開について

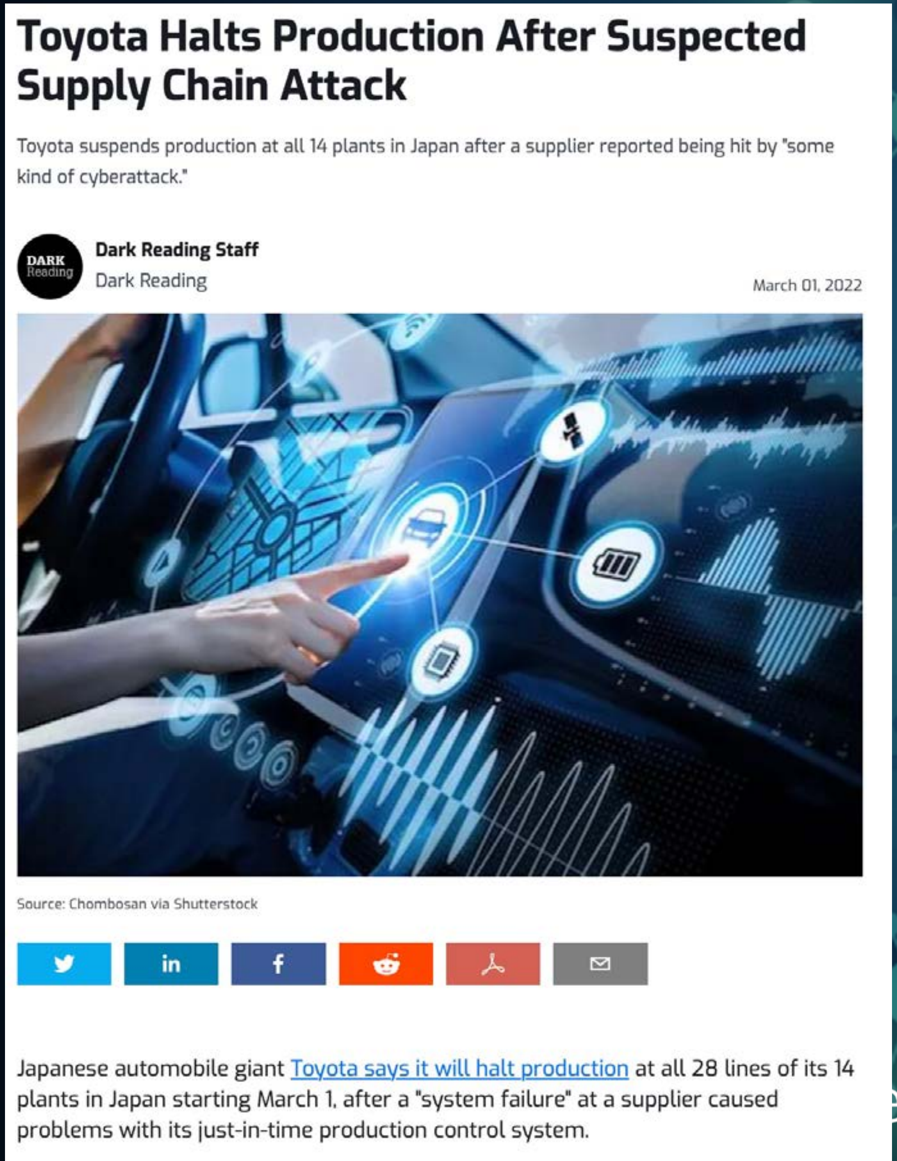
お知らせ, 工場稼働

国内仕入先（小島プレス工業株式会社）におけるシステム障害の影響を受け、本日3/1（火）の国内全14工場28ラインの稼働を停止しておりますが、明日3/2（水）1直より、すべての稼働を再開することを決定いたしました。

本日の急遽の稼働停止にあたり、お客様および仕入先、関係先の方々には、様々なご不便をお掛けしましたことを、改めてお詫び申し上げます。

関係仕入先の皆さまとともに、1日





Toyota Halts Production After Suspected Supply Chain Attack

Toyota suspends production at all 14 plants in Japan after a supplier reported being hit by "some kind of cyberattack."

Dark Reading Staff
Dark Reading
March 01, 2022

Source: Chombosan via Shutterstock

Japanese automobile giant Toyota says it will halt production at all 28 lines of its 14 plants in Japan starting March 1, after a "system failure" at a supplier caused problems with its just-in-time production control system.

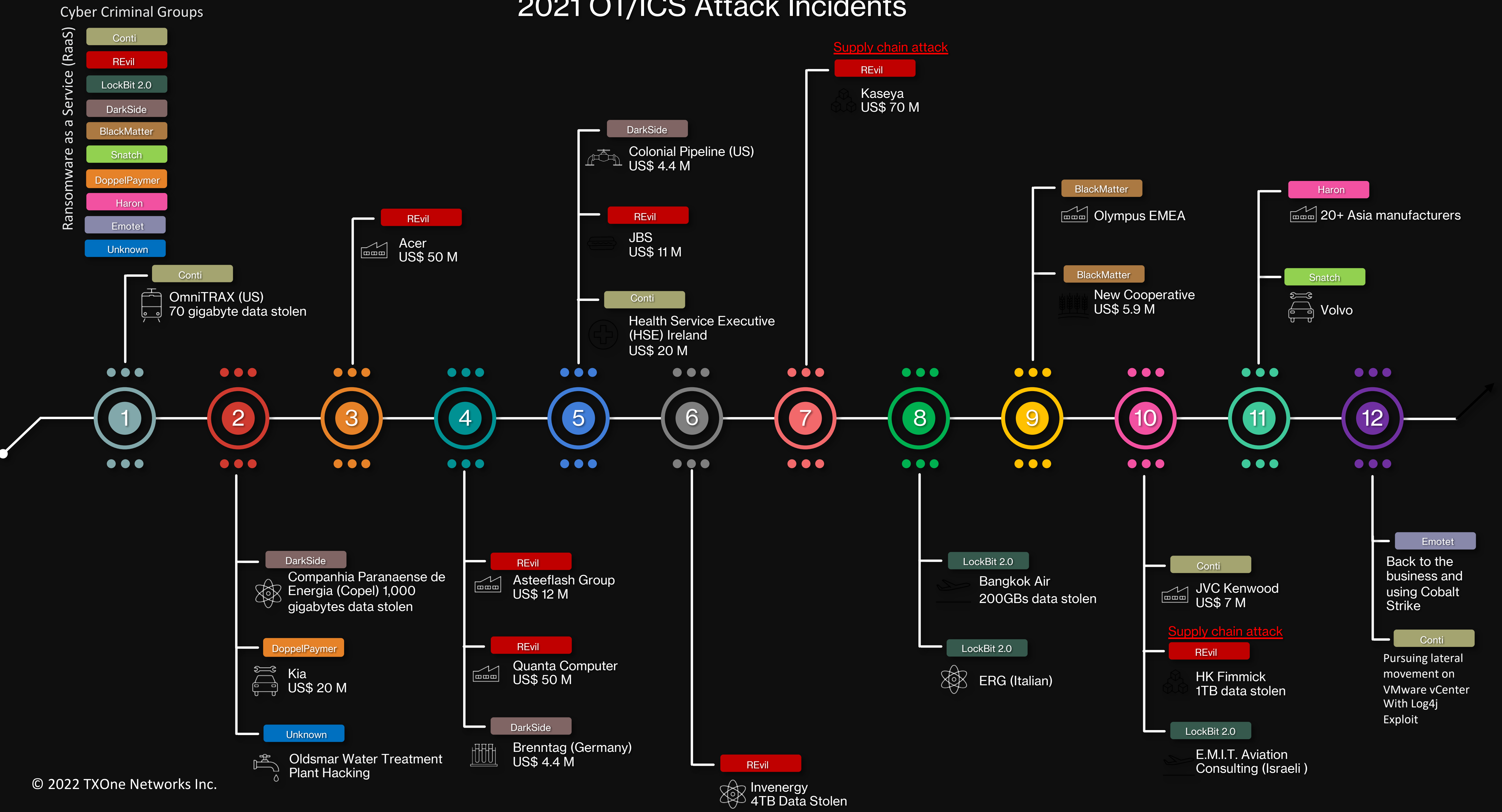
https://global.toyota/jp/newsroom/corporate/36964714.html
https://www.darkreading.com/attacks-breaches/toyota-halts-production-after-suspected-supply-chain-attack

近年遭勒索軟體攻擊現況

	2021 Q2	2021 Q3	2021 Q4	2022 Q1	From 2021 Q4 to 2022 Q1
Government	23.32%	23.58%	24.37%	21.60%	↘
Manufacturing	16.95%	15.77%	14.00%	16.46%	↗
Healthcare	12.95%	13.40%	14.92%	11.66%	↘
Technology	6.14%	7.00%	6.60%	9.14%	↗
Education	7.74%	7.67%	8.10%	8.99%	↗
Financial	7.37%	7.30%	6.74%	7.30%	↗
Retail	2.87%	2.78%	2.87%	3.14%	↗
Food and beverage	1.40%	2.59%	1.78%	2.64%	↗
Energy	1.15%	1.82%	2.99%	2.34%	↘
Transportation	2.16%	1.42%	1.66%	2.22%	↗
Banking	3.39%	2.85%	1.78%	1.93%	↗
Utilities	0.86%	1.07%	1.58%	1.57%	↘
Communication and Media	2.83%	1.29%	2.75%	1.45%	↘
Real estate	0.76%	1.23%	0.96%	1.31%	↗
Insurance	1.60%	1.54%	1.54%	1.19%	↘

txOne networks

2021 OT/ICS Attack Incidents



Cyber Criminal Groups

Ransomware as a Service (RaaS)

- Conti
- REvil
- LockBit 2.0
- DarkSide
- BlackMatter
- Snatch
- DoppelPaymer
- Haron
- Emotet
- Unknown

1

Conti
OmniTRAX (US)
70 gigabyte data stolen

2

DarkSide
Companhia Paranaense de Energia (Copel) 1,000 gigabytes data stolen

DoppelPaymer
Kia
US$ 20 M

Unknown
Oldsmar Water Treatment Plant Hacking

3

REvil
Acer
US$ 50 M

4

REvil
Asteeflash Group
US$ 12 M

REvil
Quanta Computer
US$ 50 M

DarkSide
Brenntag (Germany)
US$ 4.4 M

5

DarkSide
Colonial Pipeline (US)
US$ 4.4 M

REvil
JBS
US$ 11 M

Conti
Health Service Executive (HSE) Ireland
US$ 20 M

6

REvil
Invenergy
4TB Data Stolen

7

Supply chain attack
REvil
Kaseya
US$ 70 M

8

LockBit 2.0
Bangkok Air
200GBs data stolen

LockBit 2.0
ERG (Italian)

9

BlackMatter
Olympus EMEA

BlackMatter
New Cooperative
US$ 5.9 M

10

Conti
JVC Kenwood
US$ 7 M

Supply chain attack
REvil
HK Fimmick
1TB data stolen

LockBit 2.0
E.M.I.T. Aviation Consulting (Israeli)

11

Haron
20+ Asia manufacturers

Snatch
Volvo

12

Emotet
Back to the business and using Cobalt Strike

Conti
Pursuing lateral movement on VMware vCenter With Log4j Exploit

2021 OT/ICS Attack Incidents Highlights

Most active criminal groups in 2021

- Conti, Maze, Lockbit, REvil and DarkSide

Targeting the Critical Infrastructure and leverage supply chain attack

- Colonial Pipeline attack in May by DarkSide
- Kaseya supply chain attack by REvil

Running the RaaS business model with the affiliate programs

- Ransom demand less than 500k charge for 25%
- Ransom demand over 5M charge for 10%

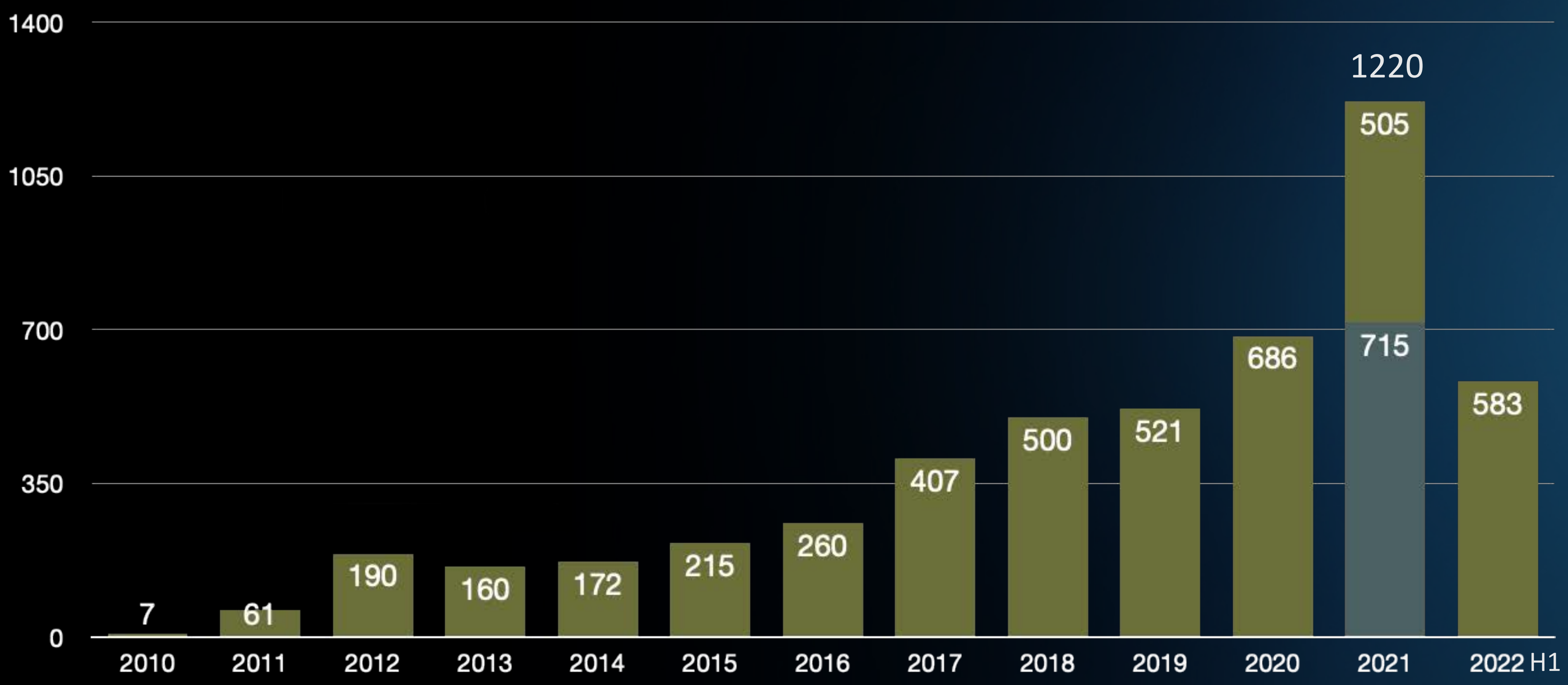
Executive Order issued by U.S. President Joe Biden

- Improving the nation’s cybersecurity
- Supply Chain and Software Bills of Materials (SBOMs)

Leverage zero-day vulnerabilities

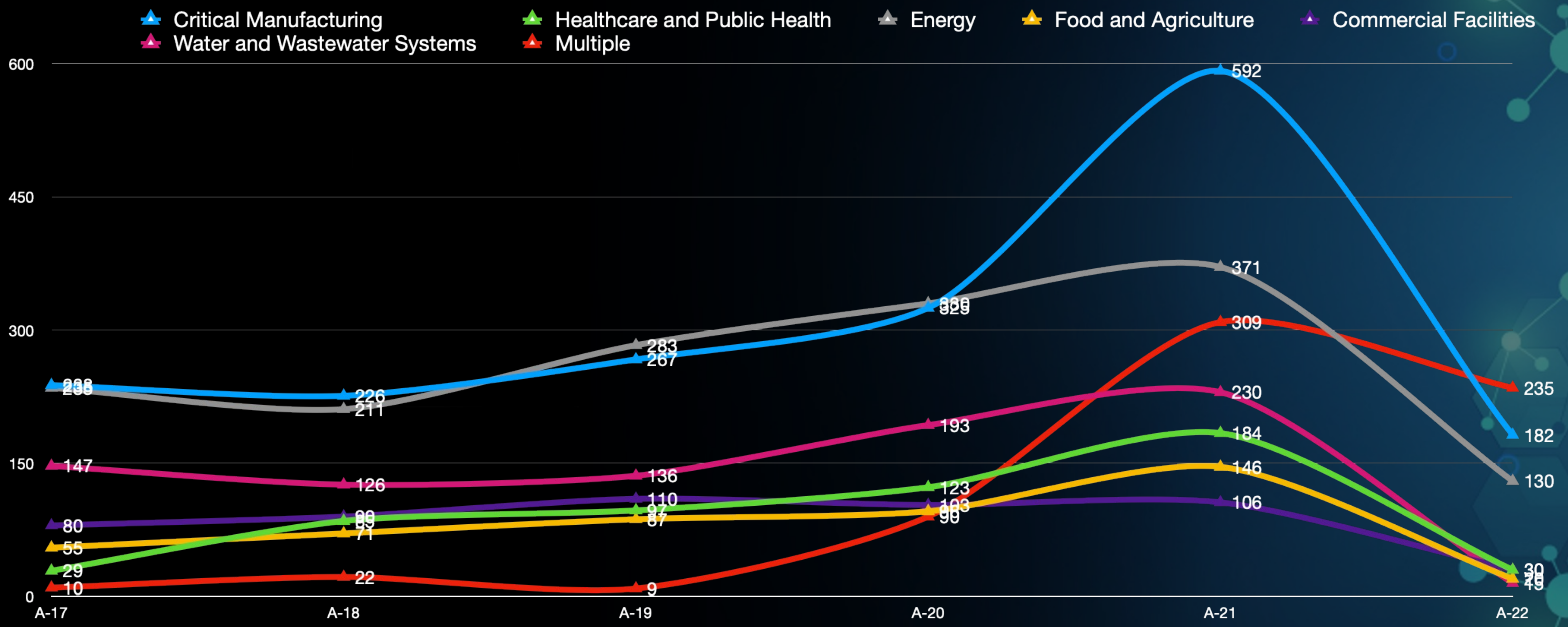
- CVE-2021-30116, Kaseya VSA vulnerability
- CVE-2021-44228, Log4J vulnerability

Recent ICS Vulnerabilities – CVE Analysis



715 CVEs in the same period last year

Recent ICS Vulnerabilities – CVE Analysis



ICS/SCADA Security Threat Situation

Vulnerabilities are mostly critical and high risk levels

The number of vulnerability is rising year by year

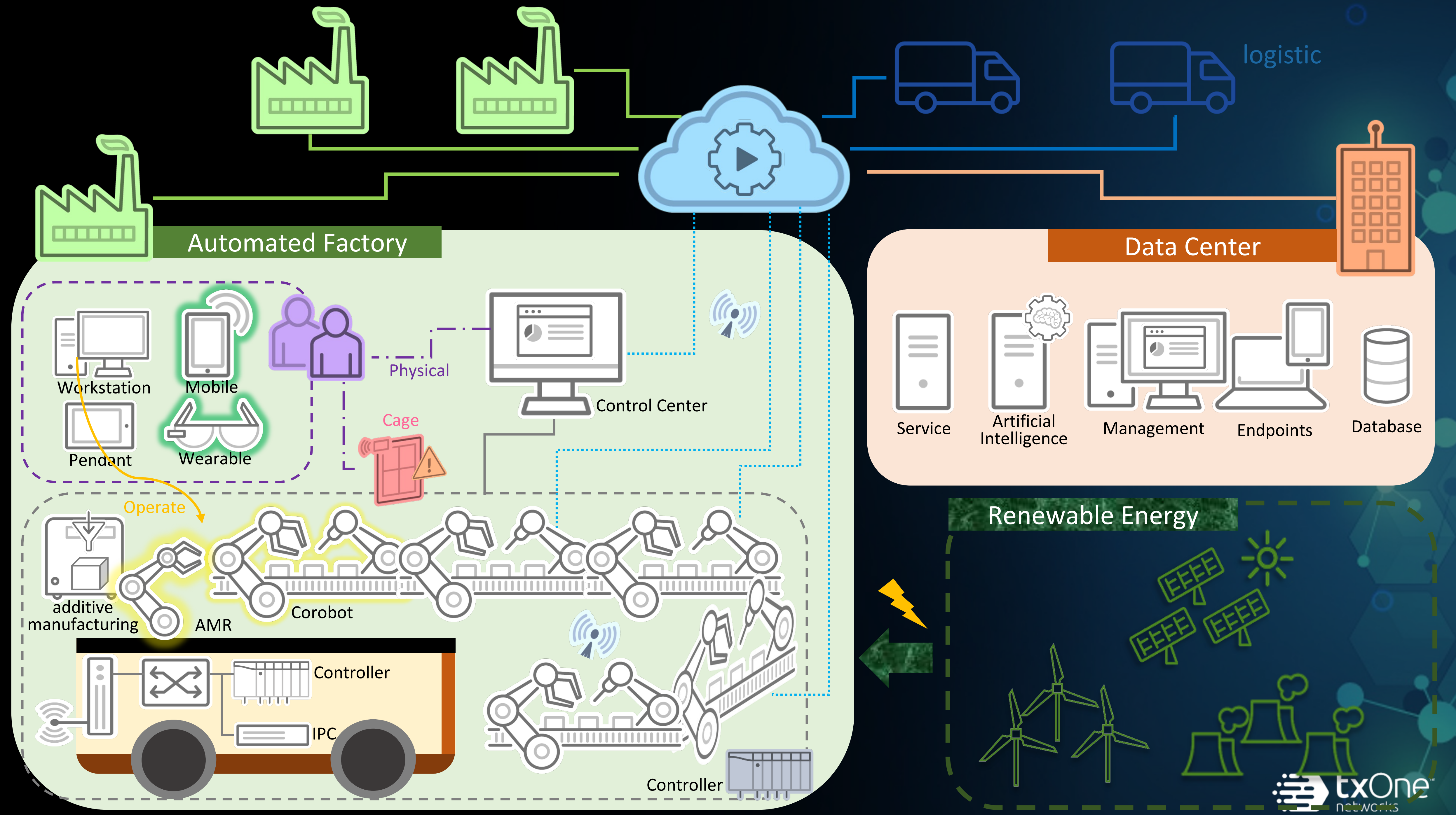
The security incidents have a huge impact

ICS/SCADA are not secure at all

Critical

txOne™ networks *The Leader of OT Zero Trust*

The Practical Attack Vectors for Modern ICS/SCADA



logistic

Automated Factory

Workstation

Mobile

Pendant

Wearable

Physical

Control Center

Cage

Operate

additive manufacturing

AMR

Corobot

Controller

IPC

Controller

Data Center

Service

Artificial Intelligence

Management

Endpoints

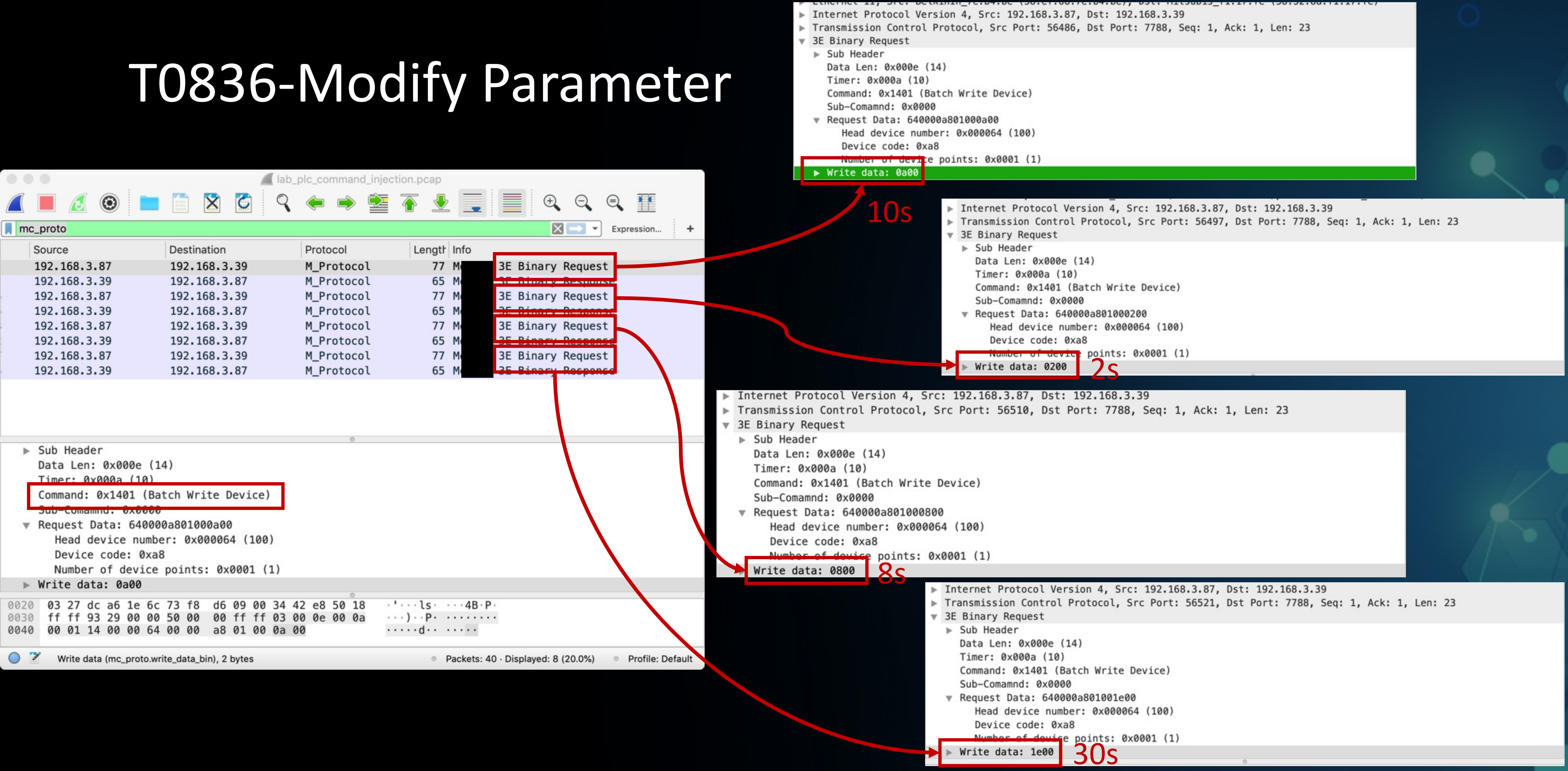
Database

Renewable Energy

Legacy ICS Protocol which Allow an Attacker Perform Command Injection to PLC

T0836-Modify Parameter with Mitsubishi Melsec Protocol

T0836-Modify Parameter



Source	Destination	Protocol	Length	Info
192.168.3.87	192.168.3.39	M_Protocol	77	M [redacted] 3E Binary Request
192.168.3.39	192.168.3.87	M_Protocol	65	M [redacted] 3E Binary Response
192.168.3.87	192.168.3.39	M_Protocol	77	M [redacted] 3E Binary Request
192.168.3.39	192.168.3.87	M_Protocol	65	M [redacted] 3E Binary Response
192.168.3.87	192.168.3.39	M_Protocol	77	M [redacted] 3E Binary Request
192.168.3.39	192.168.3.87	M_Protocol	65	M [redacted] 3E Binary Response
192.168.3.87	192.168.3.39	M_Protocol	77	M [redacted] 3E Binary Request
192.168.3.39	192.168.3.87	M_Protocol	65	M [redacted] 3E Binary Response

```
▶ Sub Header
  Data Len: 0x000e (14)
  Timer: 0x000a (10)
  Command: 0x1401 (Batch Write Device)
  Sub-Comamnd: 0x0000
▼ Request Data: 640000a801000a00
    Head device number: 0x000064 (100)
    Device code: 0xa8
    Number of device points: 0x0001 (1)
▶ Write data: 0a00
```

```
0020  03 27 dc a6 1e 6c 73 f8  d6 09 00 34 42 e8 50 18   ·'···ls· ···4B·P·
0030  ff ff 93 29 00 00 50 00  00 ff ff 03 00 0e 00 0a   ···)··P· ········
0040  00 01 14 00 00 64 00 00  a8 01 00 0a 00            ·····d·· ·····
```

Write data (mc_proto.write_data_bin), 2 bytes · Packets: 40 · Displayed: 8 (20.0%) · Profile: Default

```
▶ Internet Protocol Version 4, Src: 192.168.3.87, Dst: 192.168.3.39
▶ Transmission Control Protocol, Src Port: 56486, Dst Port: 7788, Seq: 1, Ack: 1, Len: 23
▼ 3E Binary Request
  ▶ Sub Header
    Data Len: 0x000e (14)
    Timer: 0x000a (10)
    Command: 0x1401 (Batch Write Device)
    Sub-Comamnd: 0x0000
  ▼ Request Data: 640000a801000a00
      Head device number: 0x000064 (100)
      Device code: 0xa8
      Number of device points: 0x0001 (1)
  ▶ Write data: 0a00
```

10s

```
▶ Internet Protocol Version 4, Src: 192.168.3.87, Dst: 192.168.3.39
▶ Transmission Control Protocol, Src Port: 56497, Dst Port: 7788, Seq: 1, Ack: 1, Len: 23
▼ 3E Binary Request
  ▶ Sub Header
    Data Len: 0x000e (14)
    Timer: 0x000a (10)
    Command: 0x1401 (Batch Write Device)
    Sub-Comamnd: 0x0000
  ▼ Request Data: 640000a801000200
      Head device number: 0x000064 (100)
      Device code: 0xa8
      Number of device points: 0x0001 (1)
  ▶ Write data: 0200
```

2s

```
▶ Internet Protocol Version 4, Src: 192.168.3.87, Dst: 192.168.3.39
▶ Transmission Control Protocol, Src Port: 56510, Dst Port: 7788, Seq: 1, Ack: 1, Len: 23
▼ 3E Binary Request
  ▶ Sub Header
    Data Len: 0x000e (14)
    Timer: 0x000a (10)
    Command: 0x1401 (Batch Write Device)
    Sub-Comamnd: 0x0000
  ▼ Request Data: 640000a801000800
      Head device number: 0x000064 (100)
      Device code: 0xa8
      Number of device points: 0x0001 (1)
  Write data: 0800
```

8s

```
▶ Internet Protocol Version 4, Src: 192.168.3.87, Dst: 192.168.3.39
▶ Transmission Control Protocol, Src Port: 56521, Dst Port: 7788, Seq: 1, Ack: 1, Len: 23
▼ 3E Binary Request
  ▶ Sub Header
    Data Len: 0x000e (14)
    Timer: 0x000a (10)
    Command: 0x1401 (Batch Write Device)
    Sub-Comamnd: 0x0000
  ▼ Request Data: 640000a801001e00
      Head device number: 0x000064 (100)
      Device code: 0xa8
      Number of device points: 0x0001 (1)
  ▶ Write data: 1e00
```

30s

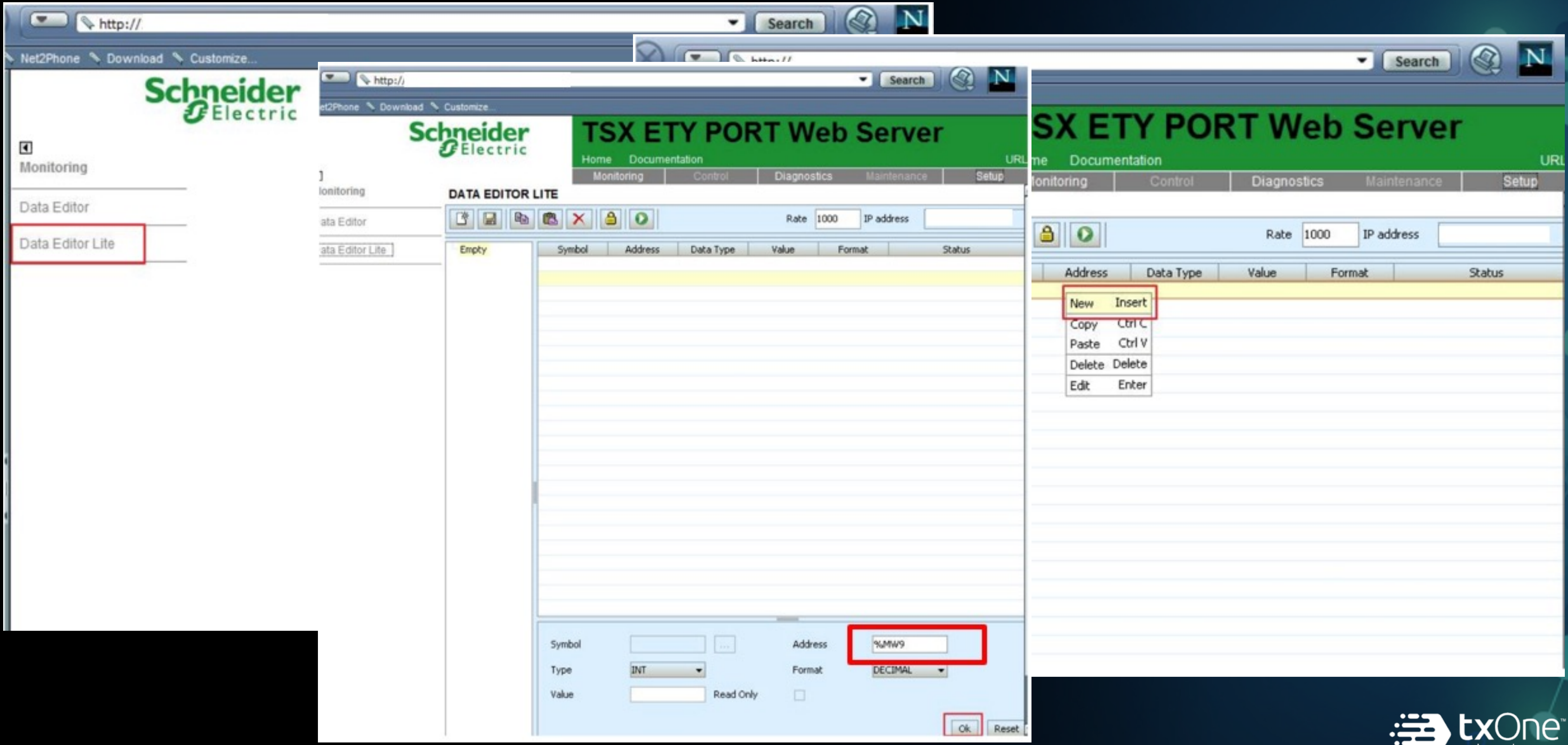
txOne networks

Legacy ICS Protocol which Allow an Attacker Perform Command Injection to HMI

T856-Spoof Reporting Message with Modbus/TCP Protocol

Web Security Flaws targeting the Control PLC

Web Security Flaws targeting the Control PLC



Rate 1000 IP address

Symbol

Type INT

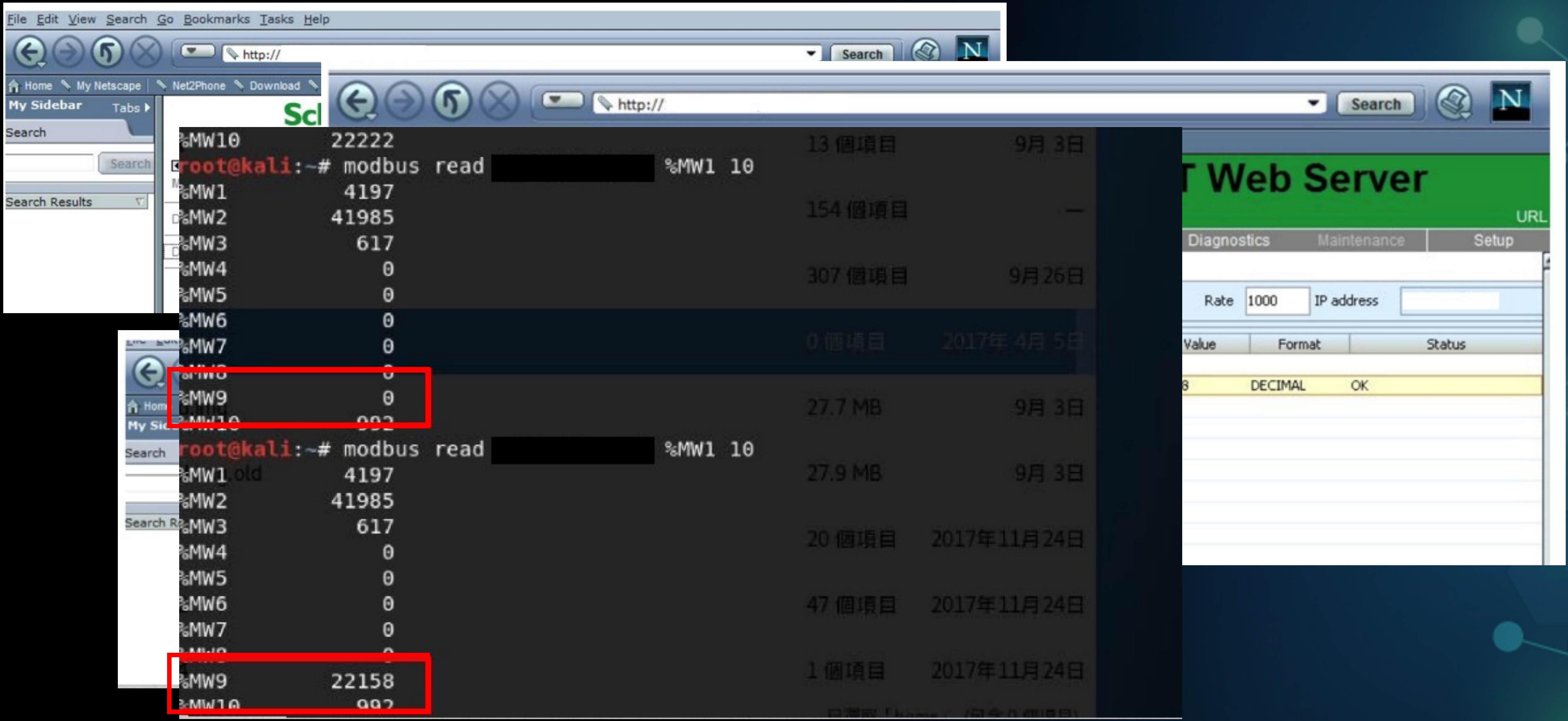
Value

Address %MW9

Format DECIMAL

Read Only □

Web Security Flaws targeting the Control PLC



```
%MW10        22222
root@kali:~# modbus read [redacted] %MW1 10
%MW1          4197
%MW2         41985
%MW3           617
%MW4             0
%MW5             0
%MW6             0
%MW7             0
%MW8             0
%MW9             0
%MW10          992
root@kali:~# modbus read [redacted] %MW1 10
%MW1          4197
%MW2         41985
%MW3           617
%MW4             0
%MW5             0
%MW6             0
%MW7             0
%MW8             0
%MW9         22158
%MW10          992
```

Web Server

Diagnostics | Maintenance | Setup

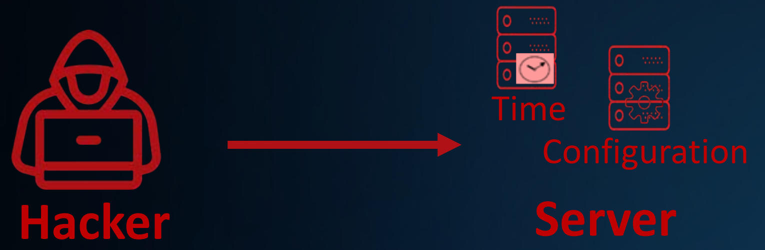
Rate 1000 IP address

Value	Format	Status
8	DECIMAL	OK

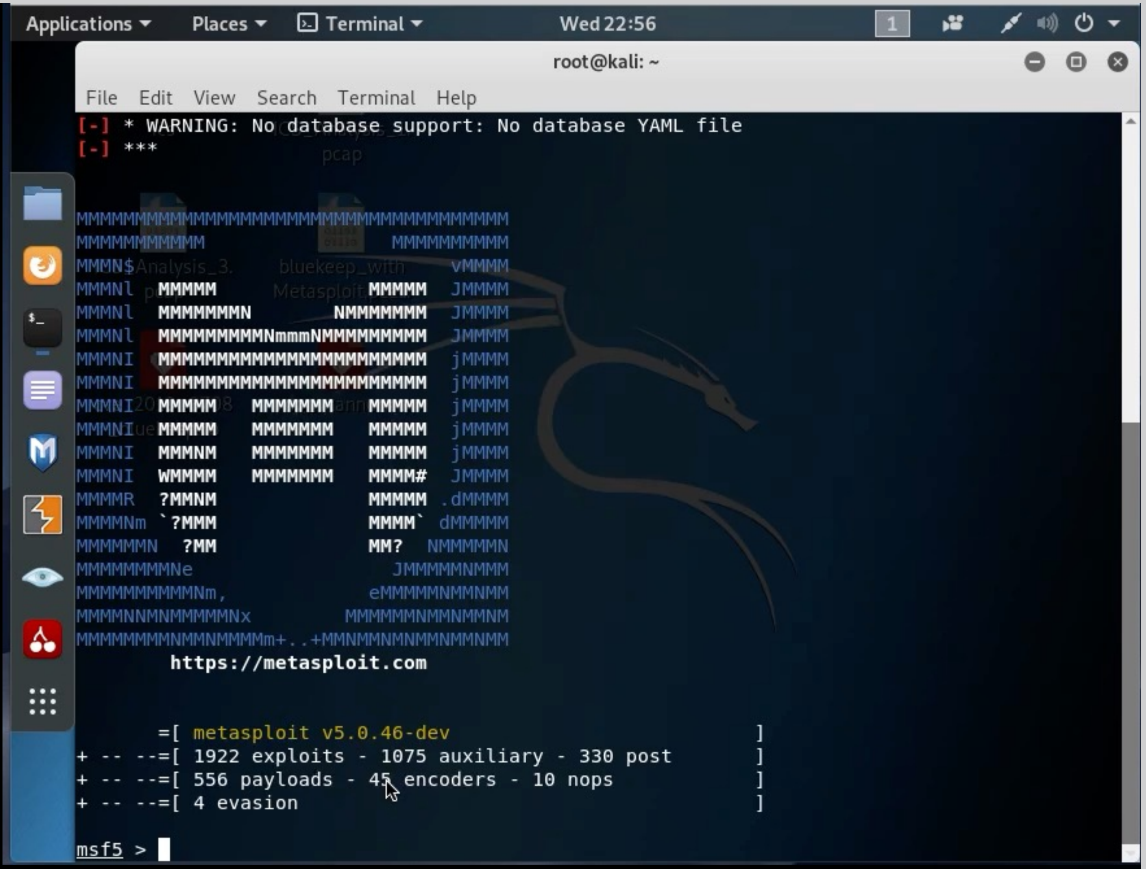
Unpatched IT Vulnerabilities in Legacy System such as Windows XP/7, Sun OS which allow attacker perform RCE attacks

Network Service Attack

BlueKeep RDP Attack



Server was compromised, and service which like time synchronization, configuration, and data exchange will fail

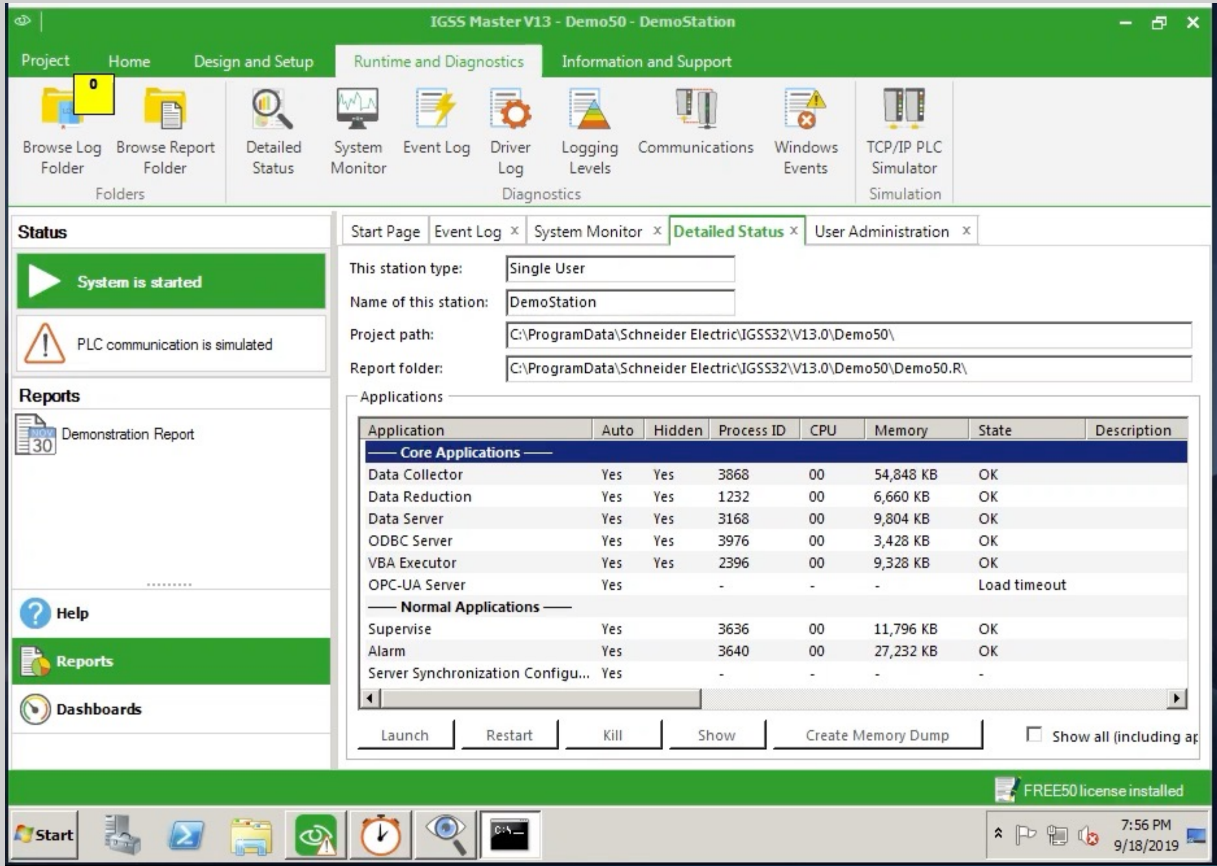

Applications ▾ Places ▾ Terminal ▾ Wed 22:56
root@kali: ~
File Edit View Search Terminal Help

```
[-] * WARNING: No database support: No database YAML file
[-] ***


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                 MMMMMMMMMMM
MMMN$                            vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v5.0.46-dev                          ]
+ -- --=[ 1922 exploits - 1075 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 >
```



Status

System is started

PLC communication is simulated

Reports

Demonstration Report

This station type: Single User

Name of this station: DemoStation

Project path: C:\ProgramData\Schneider Electric\IGSS32\V13.0\Demo50\

Report folder: C:\ProgramData\Schneider Electric\IGSS32\V13.0\Demo50\Demo50.R\

Applications

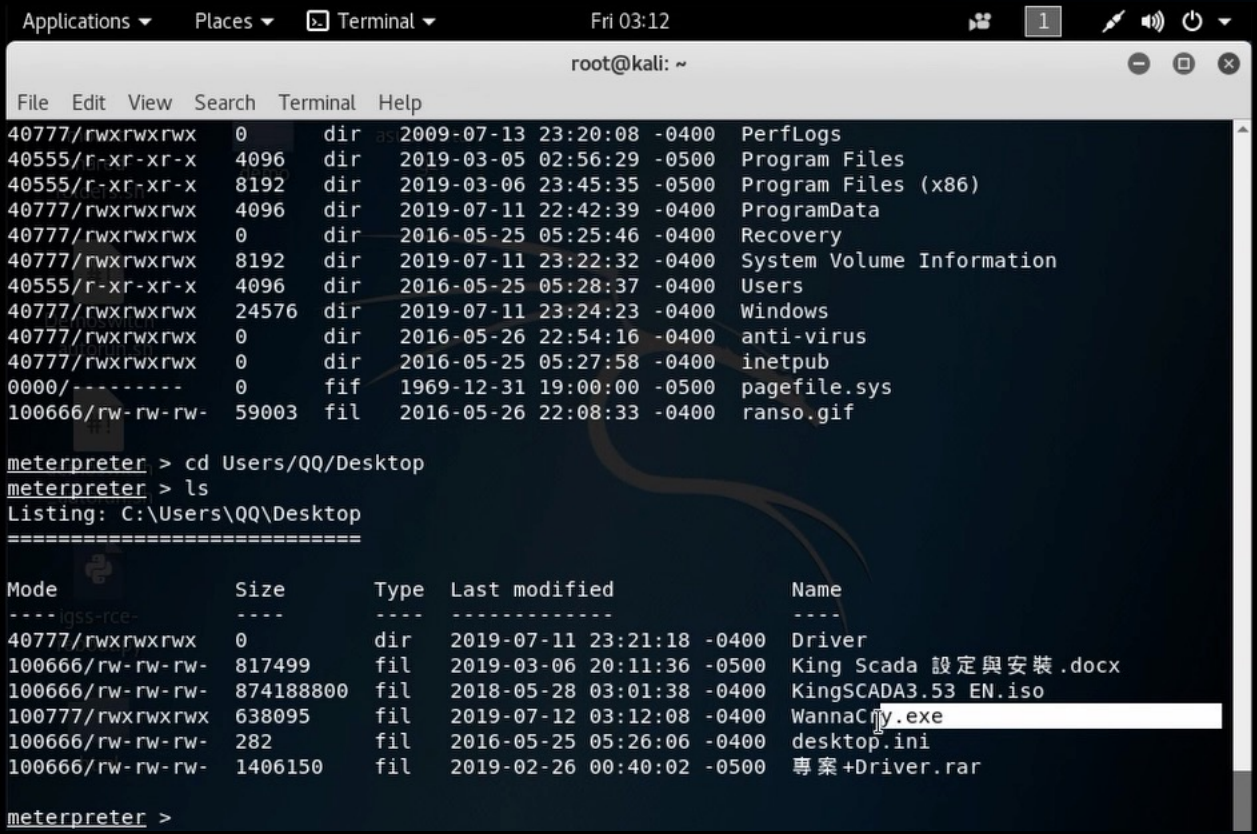
Application	Auto	Hidden	Process ID	CPU	Memory	State	Description
—— Core Applications ——							
Data Collector	Yes	Yes	3868	00	54,848 KB	OK	
Data Reduction	Yes	Yes	1232	00	6,660 KB	OK	
Data Server	Yes	Yes	3168	00	9,804 KB	OK	
ODBC Server	Yes	Yes	3976	00	3,428 KB	OK	
VBA Executor	Yes	Yes	2396	00	9,328 KB	OK	
OPC-UA Server	Yes		-	-	-	Load timeout	
—— Normal Applications ——							
Supervise	Yes		3636	00	11,796 KB	OK	
Alarm	Yes		3640	00	27,232 KB	OK	
Server Synchronization Configu...	Yes		-	-	-	-	

□ Show all (including ap

FREE50 license installed

[Potential Risk] Ransomware infection

Network Service Attack (MS17-010 and WannaCry)

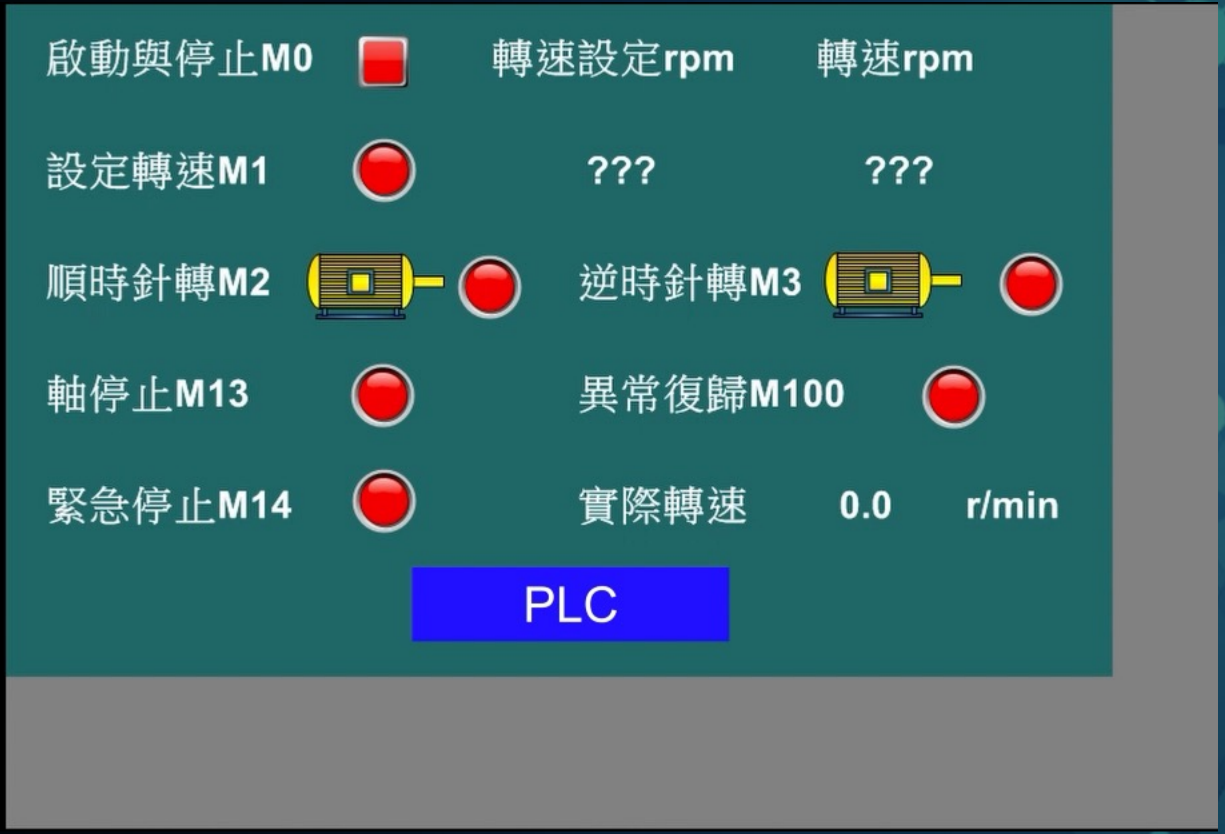


```
40777/rwxrwxrwx   0      dir   2009-07-13 23:20:08 -0400  PerfLogs
40555/r-xr-xr-x   4096   dir   2019-03-05 02:56:29 -0500  Program Files
40555/r-xr-xr-x   8192   dir   2019-03-06 23:45:35 -0500  Program Files (x86)
40777/rwxrwxrwx   4096   dir   2019-07-11 22:42:39 -0400  ProgramData
40777/rwxrwxrwx   0      dir   2016-05-25 05:25:46 -0400  Recovery
40777/rwxrwxrwx   8192   dir   2019-07-11 23:22:32 -0400  System Volume Information
40555/r-xr-xr-x   4096   dir   2016-05-25 05:28:37 -0400  Users
40777/rwxrwxrwx   24576  dir   2019-07-11 23:24:23 -0400  Windows
40777/rwxrwxrwx   0      dir   2016-05-26 22:54:16 -0400  anti-virus
40777/rwxrwxrwx   0      dir   2016-05-25 05:27:58 -0400  inetpub
0000/---------    0      fif   1969-12-31 19:00:00 -0500  pagefile.sys
100666/rw-rw-rw-  59003  fil   2016-05-26 22:08:33 -0400  ranso.gif

meterpreter > cd Users/QQ/Desktop
meterpreter > ls
Listing: C:\Users\QQ\Desktop
============================

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
40777/rwxrwxrwx   0          dir   2019-07-11 23:21:18 -0400  Driver
100666/rw-rw-rw-  817499     fil   2019-03-06 20:11:36 -0500  King Scada 設定與安裝.docx
100666/rw-rw-rw-  874188800  fil   2018-05-28 03:01:38 -0400  KingSCADA3.53 EN.iso
100777/rwxrwxrwx  638095     fil   2019-07-12 03:12:08 -0400  WannaCry.exe
100666/rw-rw-rw-  282        fil   2016-05-25 05:26:06 -0400  desktop.ini
100666/rw-rw-rw-  1406150    fil   2019-02-26 00:40:02 -0500  專案+Driver.rar

meterpreter >
```



[Potential Risk]
Time-sync attack via NTP Server by GPS Spoofing

GPS Spoofing by HackRF

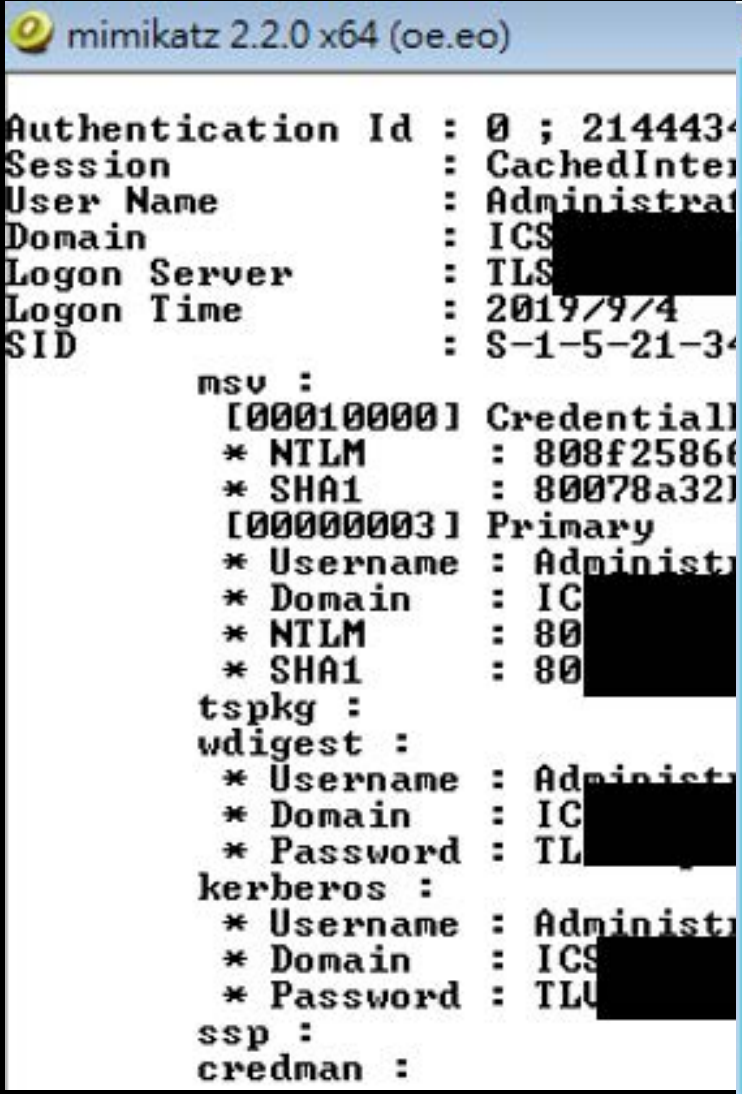
TXOne Networks Inc.

USB Attack to Disrupt Operation

Physical Attack with Bad USB

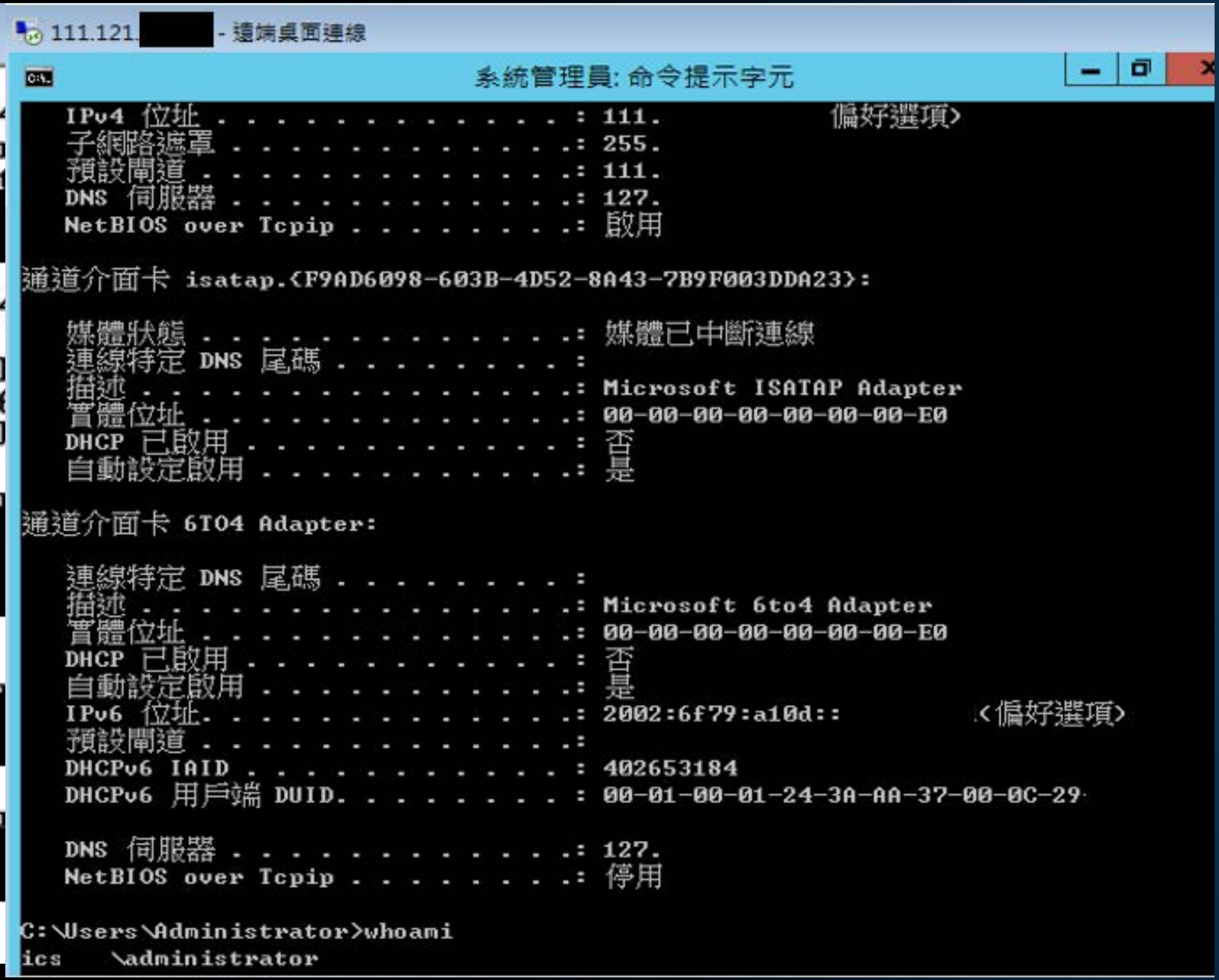
TXOne Networks Inc.

Dump Memory



mimikatz 2.2.0 x64 (oe.eo)

```
Authentication Id : 0 ; 214443
Session           : CachedInter
User Name         : Administrat
Domain            : ICS[redacted]
Logon Server      : TLS
Logon Time        : 2019/9/4
SID               : S-1-5-21-3
        msv :
         [00010000] Credentiall
         * NTLM     : 808f2586
         * SHA1     : 80078a32
         [00000003] Primary
         * Username : Administ
         * Domain   : IC[redacted]
         * NTLM     : 80
         * SHA1     : 80
        tspkg :
        wdigest :
         * Username : Administ
         * Domain   : IC[redacted]
         * Password : TL
        kerberos :
         * Username : Administ
         * Domain   : ICS[redacted]
         * Password : TLU
        ssp :
        credman :
```



111.121.[redacted] - 遠端桌面連線

系統管理員: 命令提示字元

```
   IPv4 位址 . . . . . . . . . . . . : 111.          偏好選項)
   子網路遮罩 . . . . . . . . . . . .: 255.
   預設閘道 . . . . . . . . . . . . .: 111.
   DNS 伺服器 . . . . . . . . . . . .: 127.
   NetBIOS over Tcpip . . . . . . . .: 啟用

通道介面卡 isatap.{F9AD6098-603B-4D52-8A43-7B9F003DDA23}:

   媒體狀態 . . . . . . . . . . . . .: 媒體已中斷連線
   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . .: Microsoft ISATAP Adapter
   實體位址 . . . . . . . . . . . . .: 00-00-00-00-00-00-00-E0
   DHCP 已啟用 . . . . . . . . . . . : 否
   自動設定啟用 . . . . . . . . . . .: 是

通道介面卡 6TO4 Adapter:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . .: Microsoft 6to4 Adapter
   實體位址 . . . . . . . . . . . . .: 00-00-00-00-00-00-00-E0
   DHCP 已啟用 . . . . . . . . . . . : 否
   自動設定啟用 . . . . . . . . . . .: 是
   IPv6 位址. . . . . . . . . . . . .: 2002:6f79:a10d::          (偏好選項)
   預設閘道 . . . . . . . . . . . . .:
   DHCPv6 IAID . . . . . . . . . . . : 402653184
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-3A-AA-37-00-0C-29

   DNS 伺服器 . . . . . . . . . . . .: 127.
   NetBIOS over Tcpip . . . . . . . .: 停用

C:\Users\Administrator>whoami
ics    \administrator
```

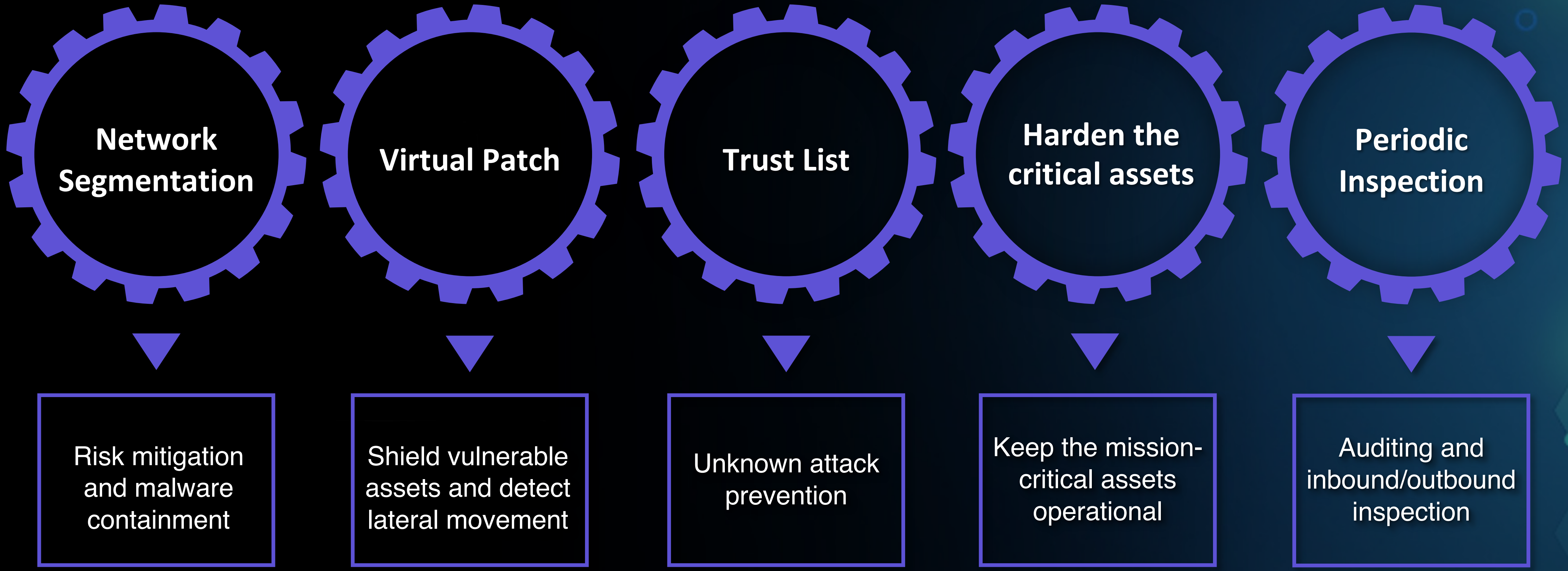
針對自動化工廠的潛在威脅

- 高度數位化的工廠將大量的**機械連上網路**，使 Internet Accessible Device 或 Wireless Compromise等 Initial Access 的攻擊技術出現於工廠環境之中
- 工業機器人開發環境擁有遭**混入惡意程式的風險**，使具有高權限的工作站存在執行惡意行為的威脅
- 保管不當的 Augmented Reality裝置，可能使工廠**機密資料遭竊取**，甚至使雲端資料遭破壞
- Additive Manufacturing設備由於其運作方式，當**設定檔遭攻擊者竄**改可能導致設備燃燒，造成工廠大規模的災害

txOne™ networks *The Leader of OT Zero Trust*

The Common Defense Strategies for Securing Read-World ICS Environment

Best Practices for ICS Cybersecurity Resilience



Network Segmentation

Risk mitigation and malware containment

Virtual Patch

Shield vulnerable assets and detect lateral movement

Trust List

Unknown attack prevention

Harden the critical assets

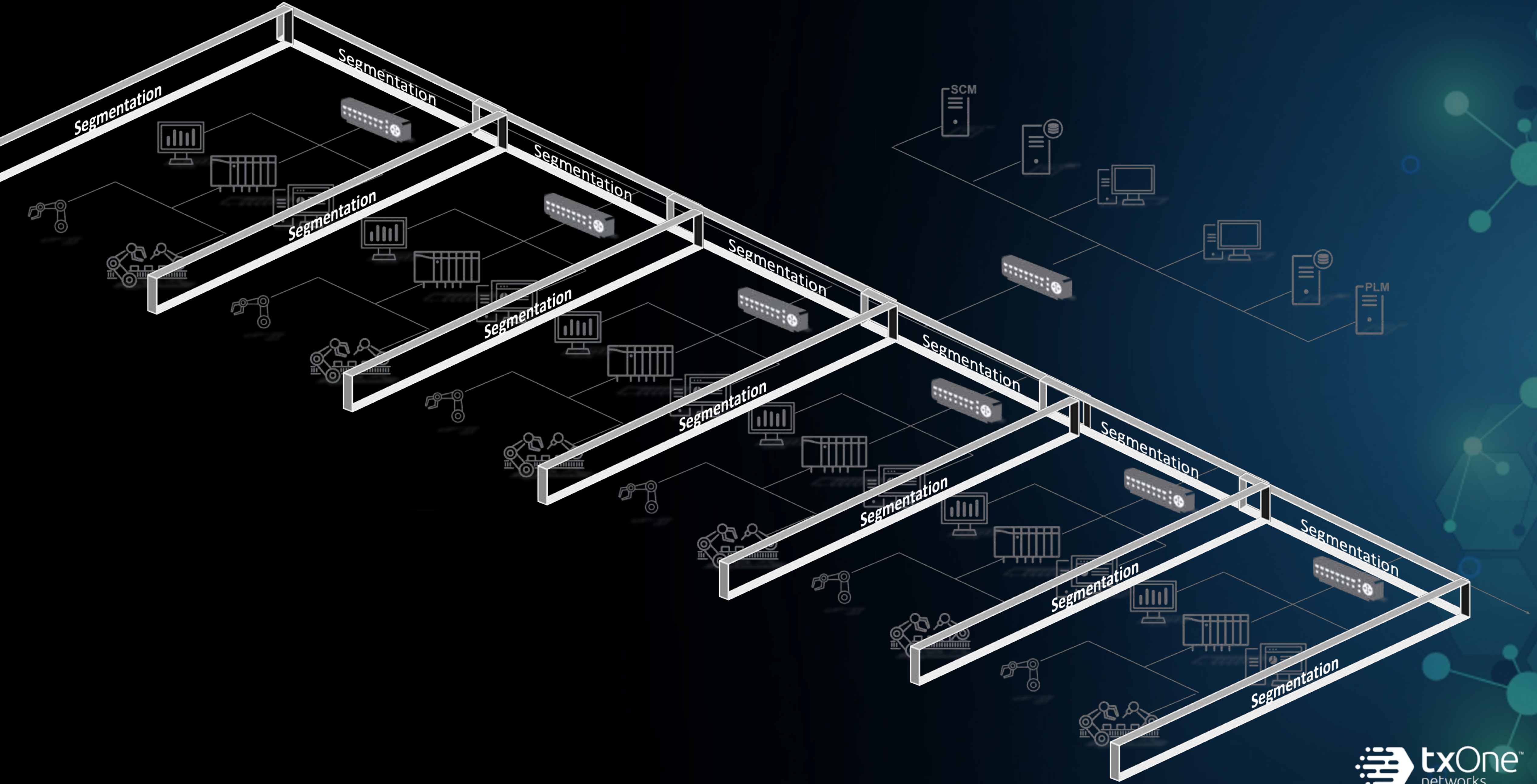
Keep the mission-critical assets operational

Periodic Inspection

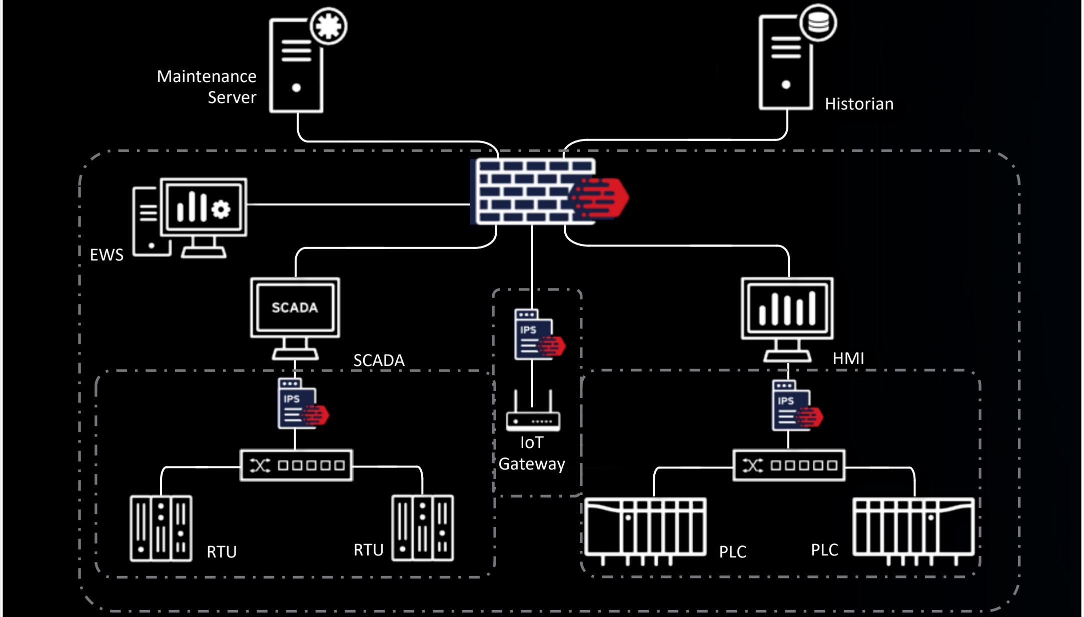
Auditing and inbound/outbound inspection

txOne networks

Network Segmentation

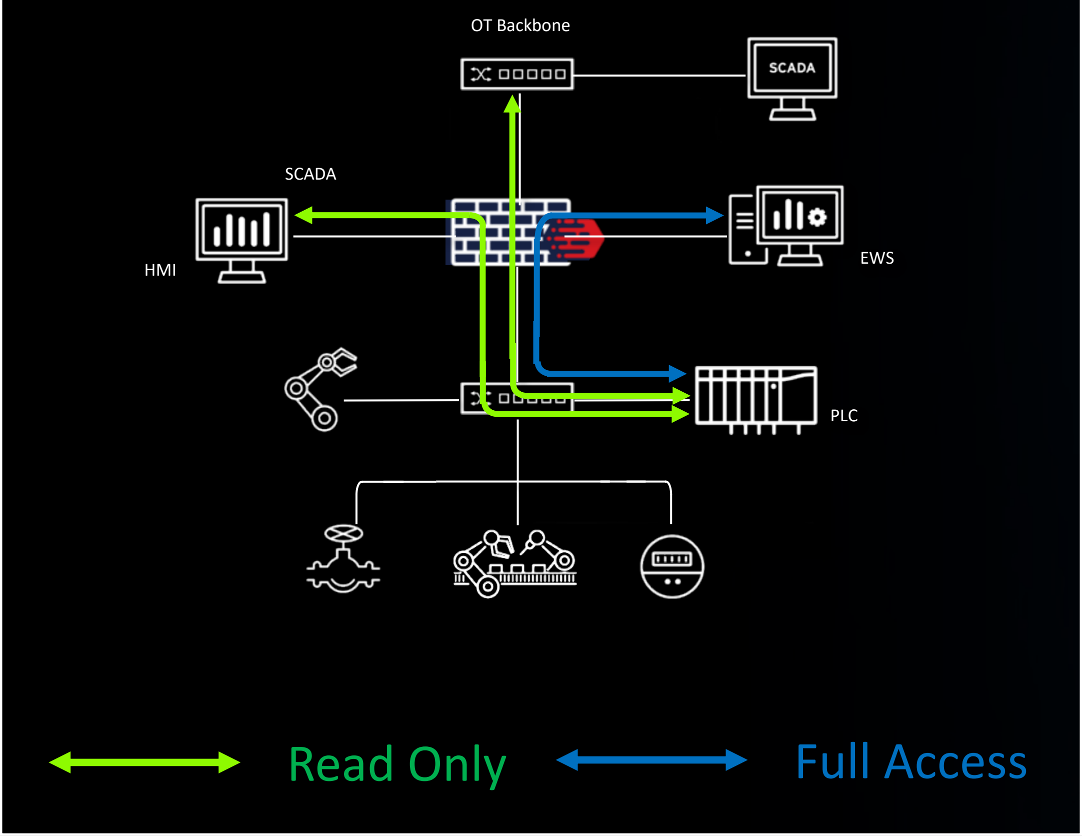


Effective Internal/Micro Segmentation and Shielding with Virtual Patch



- Divide a big flat L2 network into secured segments
- Virtual Patch (IPS)
  - Containment of malware and worms
  - Shield device vulnerabilities
  - Deeply inspect IT protocols: SMB, RDP, …
- Industrial-Grade Hardware

Trust List



- Asset and protocol visibility
- Fine-grained access control at different levels
  - Devices
  - Protocols (HL7, DICOM, Modbus, Melsec/SLMP, CC-Link IE, Ethernet/IP, Profinet, S7COMM, HSMS/SECS-II, …)
  - Control Commands (read, configure, shutdown, …)
- Greatly lower the possibility of Denial-of-Service by OT trojans