MANDIANT®

OT/ICS Threats

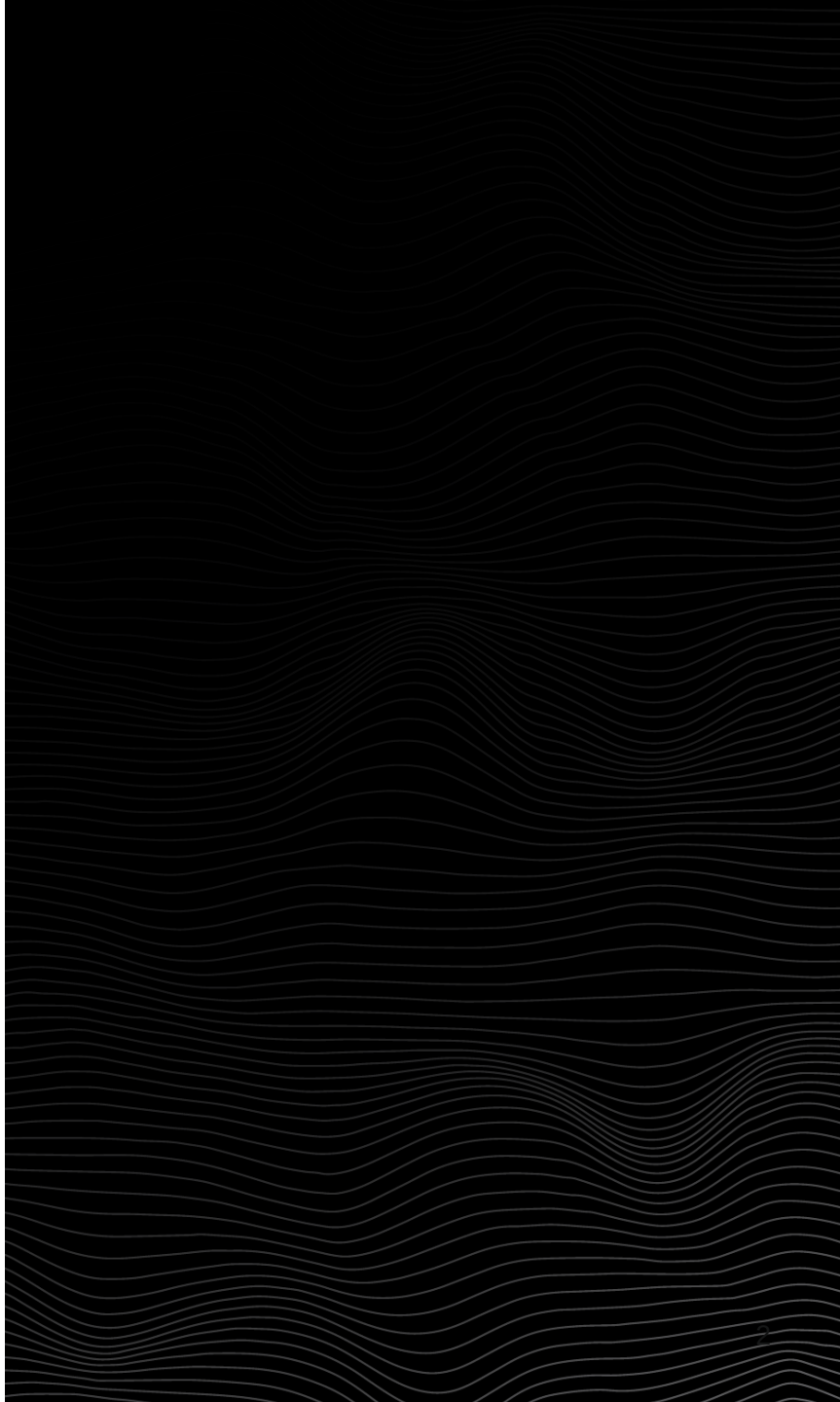
IAEC

German Simkin

July 2022

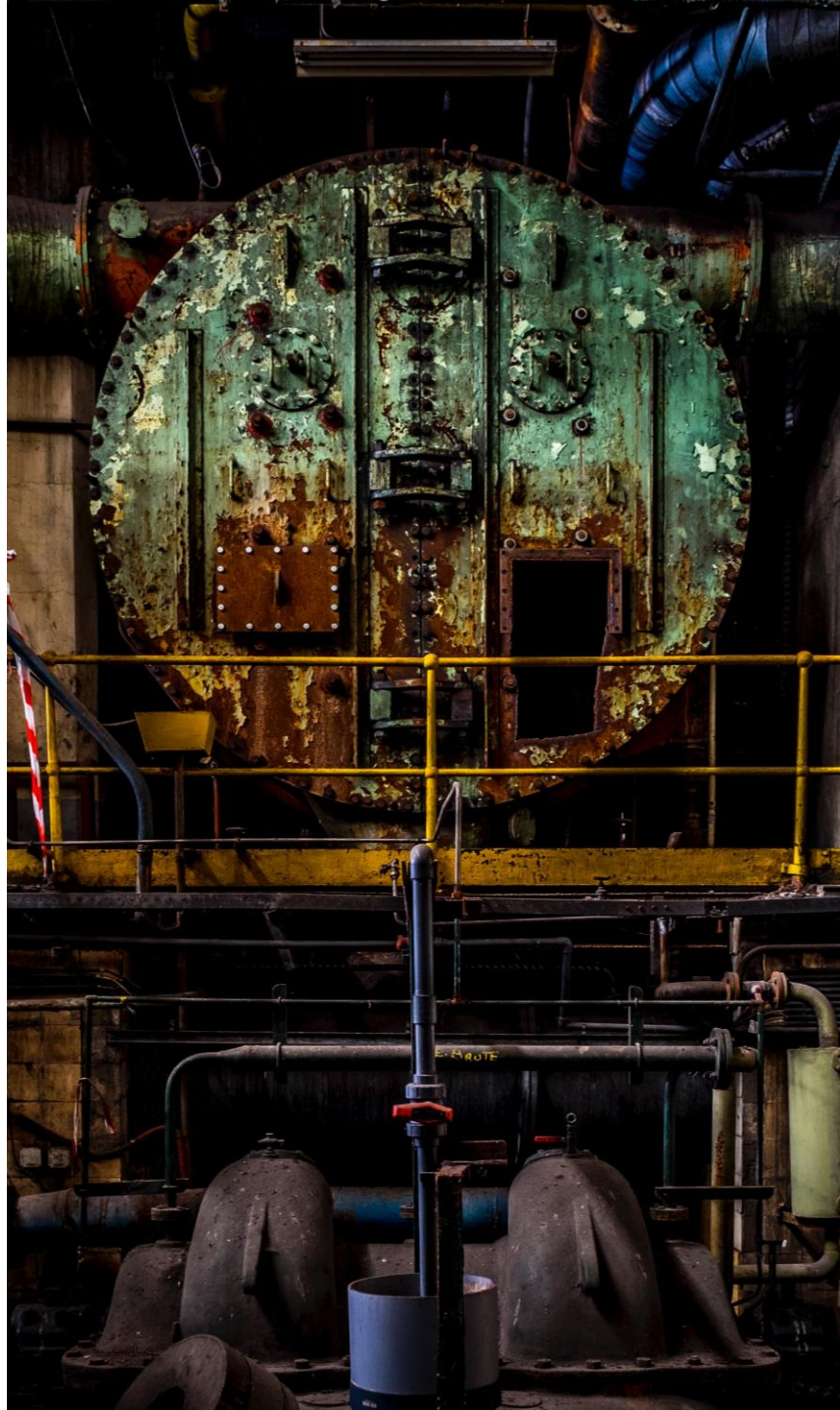
Agenda

- Intro
- Timeline
- Recent threats and capabilities
- Vulnerability and mitigation



Overview

- Cyber threats are increasing in sophistication and volume – ICS/OT is not immune.
- State sponsored actors, cyber criminals, and hacktivists all have track records of targeting ICS/OT.
- Body of evidence indicates ICS/OT systems can be particularly vulnerable to cyber threats.
- State sponsored actors view cyber-attacks on ICS/OT as crucial for war planning.



Risks

- Intermediary systems as a steppingstone to gain access to ICS/OT systems
  - ICS/OT targeted hacking tools
  - Increased risk from interconnected networks

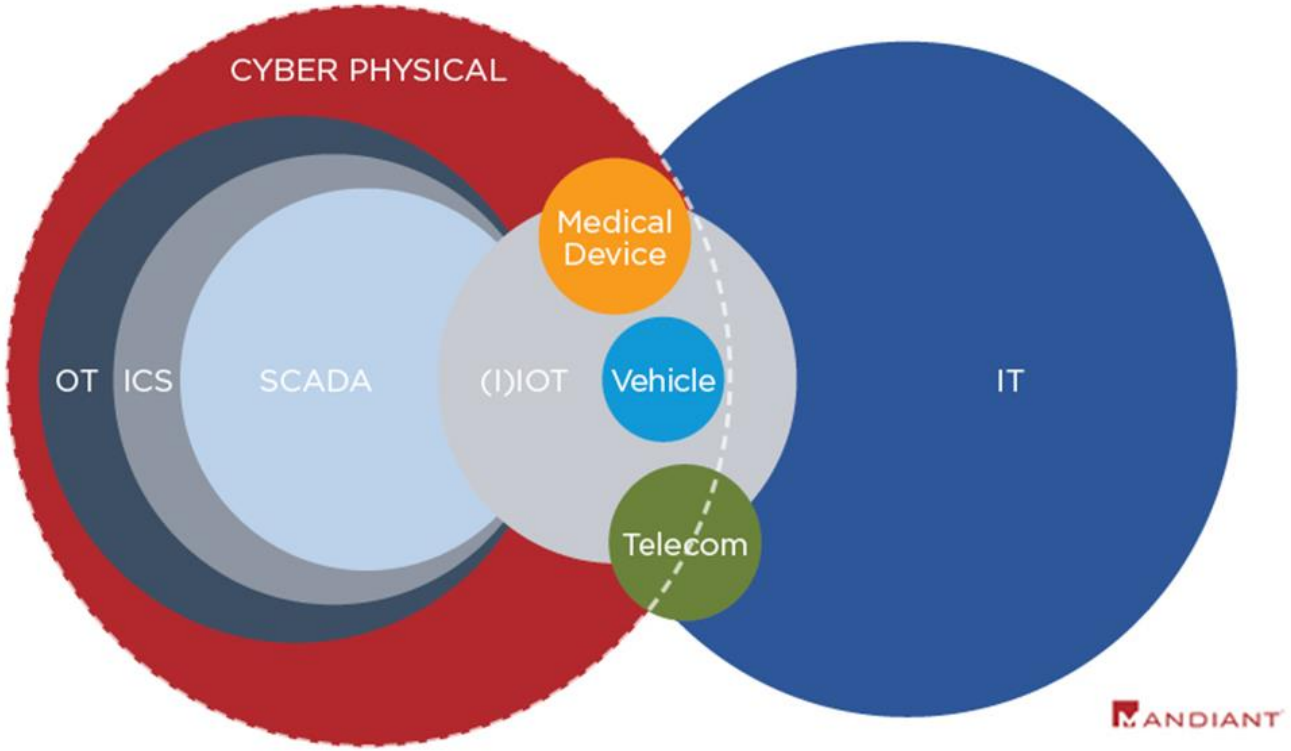
- Legacy devices and systems particularly vulnerable
  - Longer lifecycle than traditional IT
  - Low bandwidth may not support additional security mechanisms

- Insecure protocols inherent in some ICS/OT systems:
  - Modbus
  - Niagara Fox

Cyber Physical Intelligence

- Cyber physical intelligence is evidence-based knowledge and analysis about existing or emerging threats or hazards to cyber physical systems, such as operational technology (OT), industrial control systems (ICS), medical devices, vehicles, and different types of telecommunications.

- Mandiant's cyber physical reporting integrates data and analysis from across Mandiant and FireEye—including frontline data from consulting engagements, our Managed Defense (MD) security operations center (SOC) investigations, product telemetry, monitoring of and engaging with threat actors, among other sources.



CATEGORIES FOR MANDIANT THREAT INTELLIGENCE'S OT-CSIO

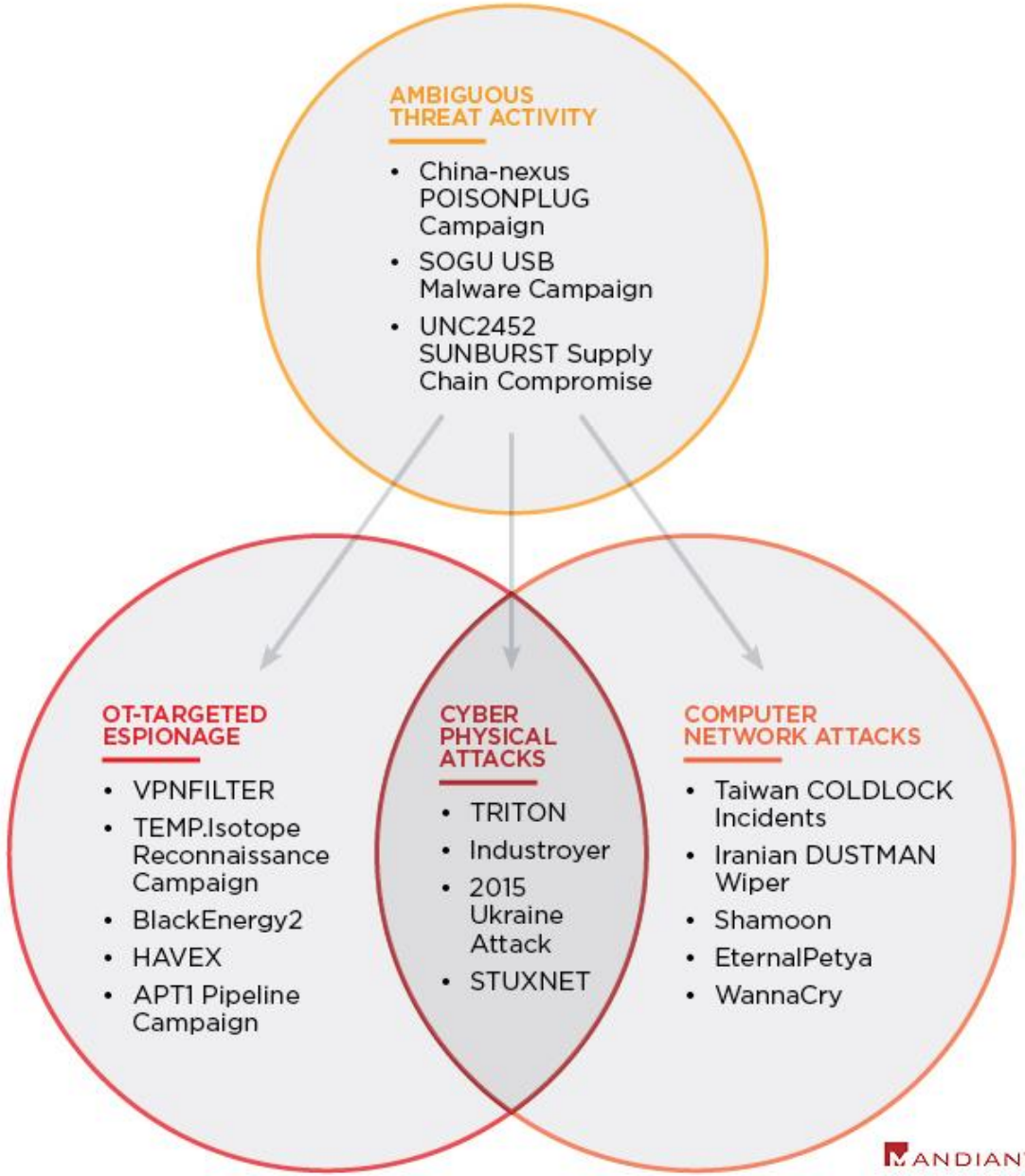
CATEGORY	CLASS	DESCRIPTION
Target	ICS-targeted	Specifically targets ICS
	Non-targeted	Collaterally or coincidentally impacts ICS
Sophistication	Low	Based on TTPs, context, previous acts, vulnerabilities exploited, detectability, etc.
	Medium	
	High	
Impact	System Compromise	Non-public data is accessed
	Data Theft	Non-public data is stolen
	Degradation	Cyber and/or physical systems' standard operations are negatively impacted, but not disrupted
	Disruption	Cyber and/or physical systems' operations are interrupted
	Destruction	Physical systems are destroyed or severely damaged
Impacted Equipment	Corporate (Zone 4/5)	E.g., Computer, Printer
	Plant DMZ (Zone 3.5)	E.g., Application Server, Historian
	ICS/Supervisory (Zone 2/3)	E.g., HMI, SCADA, Historian
	Control (Zone 1)	E.g., PLC, Controller, RTU, PAC
	Process (Zone 0)	E.g., Sensor, Actuator
	Safety	E.g., PLC, Relay, Sensor

MANDIANT

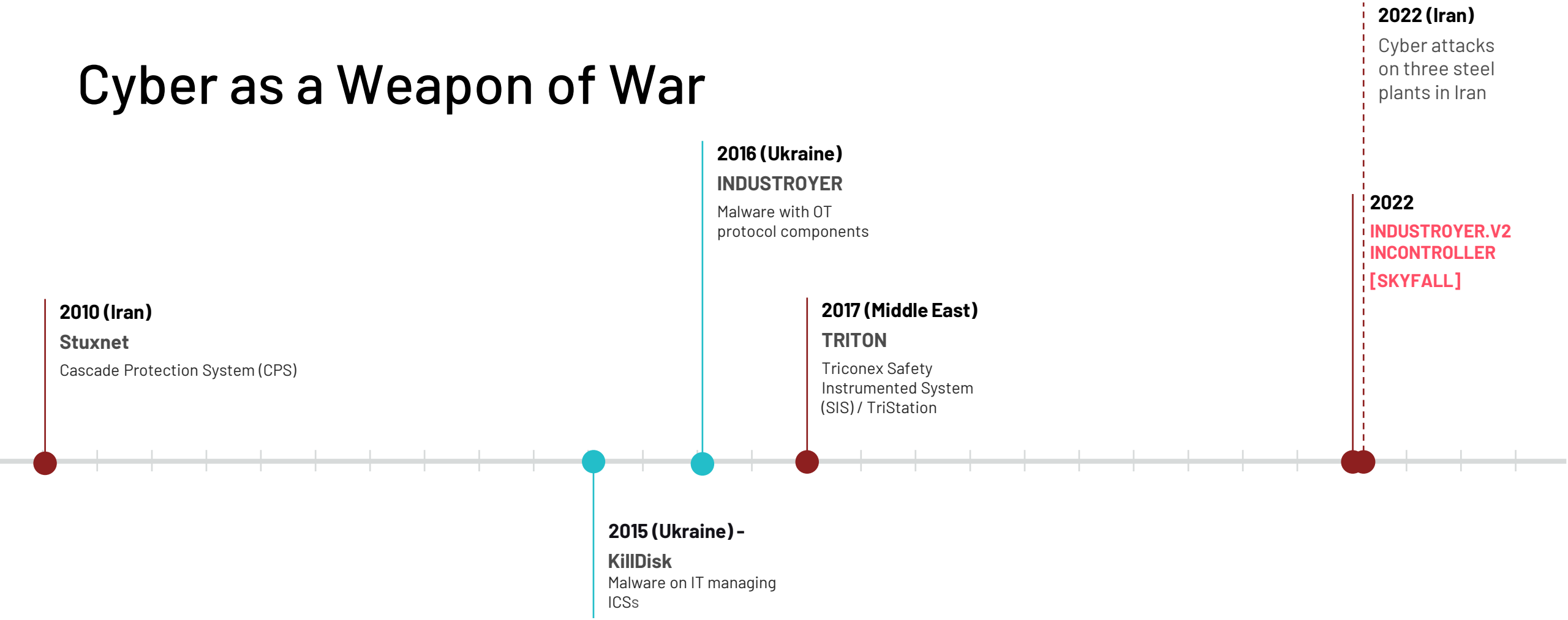
ICS Key Incidents Timeline

Maroochy Sewage Spill	2001	
	2002	
	2003	North East Blackout
	2004	
	2005	
	2006	
Aurora Generator Test	2007	
	2008	CIA Reports Foreign Utilities Hacks
	2009	
Stuxnet	2010	
	2011	Duqu
Shamoon	2012	
	2013	Havex
Port Hudson Paper Mill Insider Threat	2014	
		Iranian Targeting of Western Airports
BlackEnergy 3: Ukraine Blackout (Sandworm Team)	2015	
	2016	Industroyer: Ukraine Blackout (Sandworm Team)
WannaCry Ransomware	2017	
		NotPetya
EaternalPetya Ransomware		
		BadRabbit Ransomware
TEMP.Isotope Campaign		
	2018	TRITON: TEMP.Veles Triconex Safety Systems Malfunction
Olympic Destroyer		
	2019	LockerGoga Ransomware

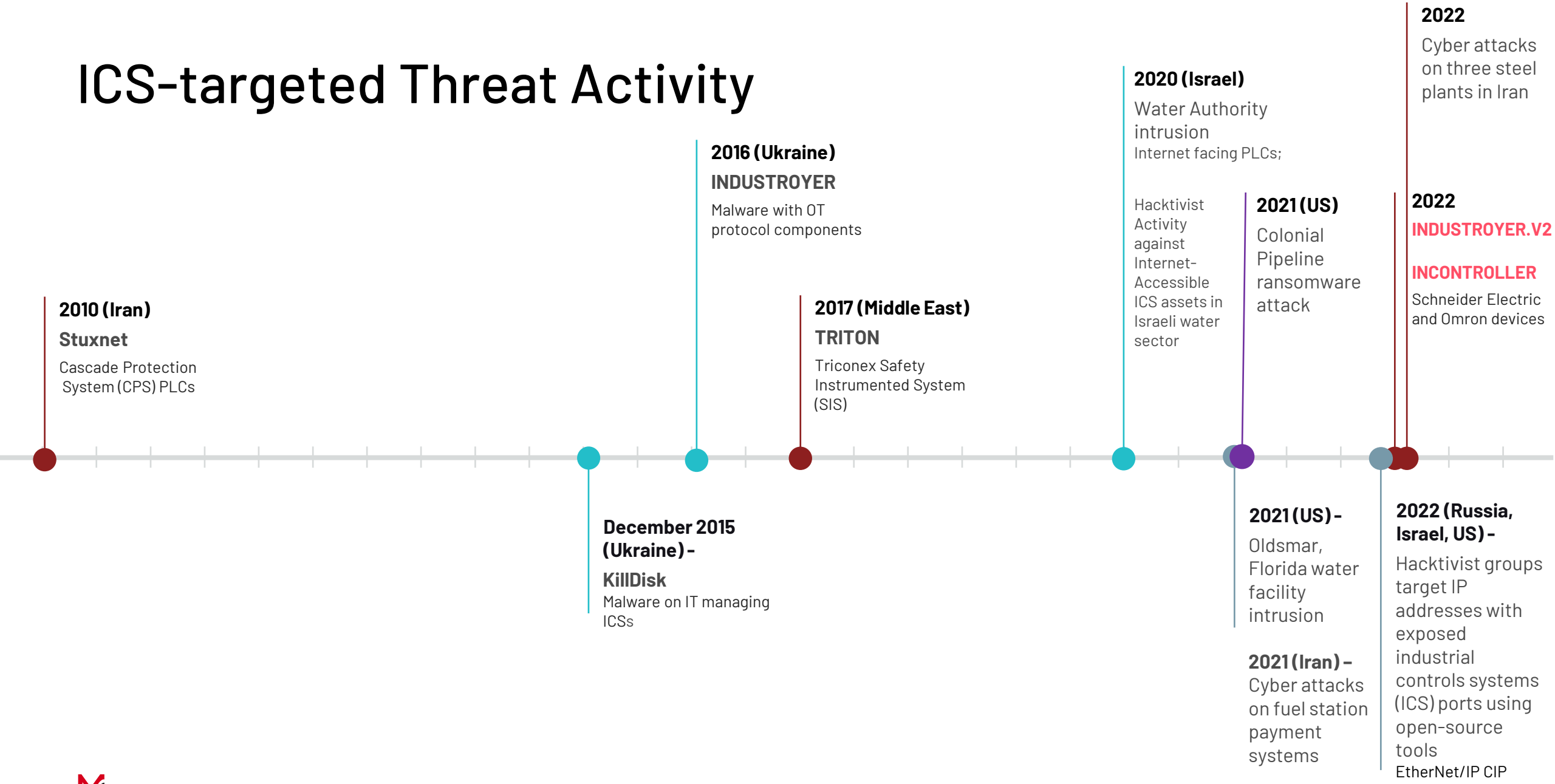
State-Sponsored Cyber Threat Activity



Cyber as a Weapon of War



ICS-targeted Threat Activity



Weapons

INCONTROLLER

Likely State-Sponsored Malware

ICONTROLLER is a set of, likely state sponsored, ICS-oriented attack tools built to target specific **Schneider Electric** and **Omron** devices embedded in different types of machinery leveraged across multiple industries.

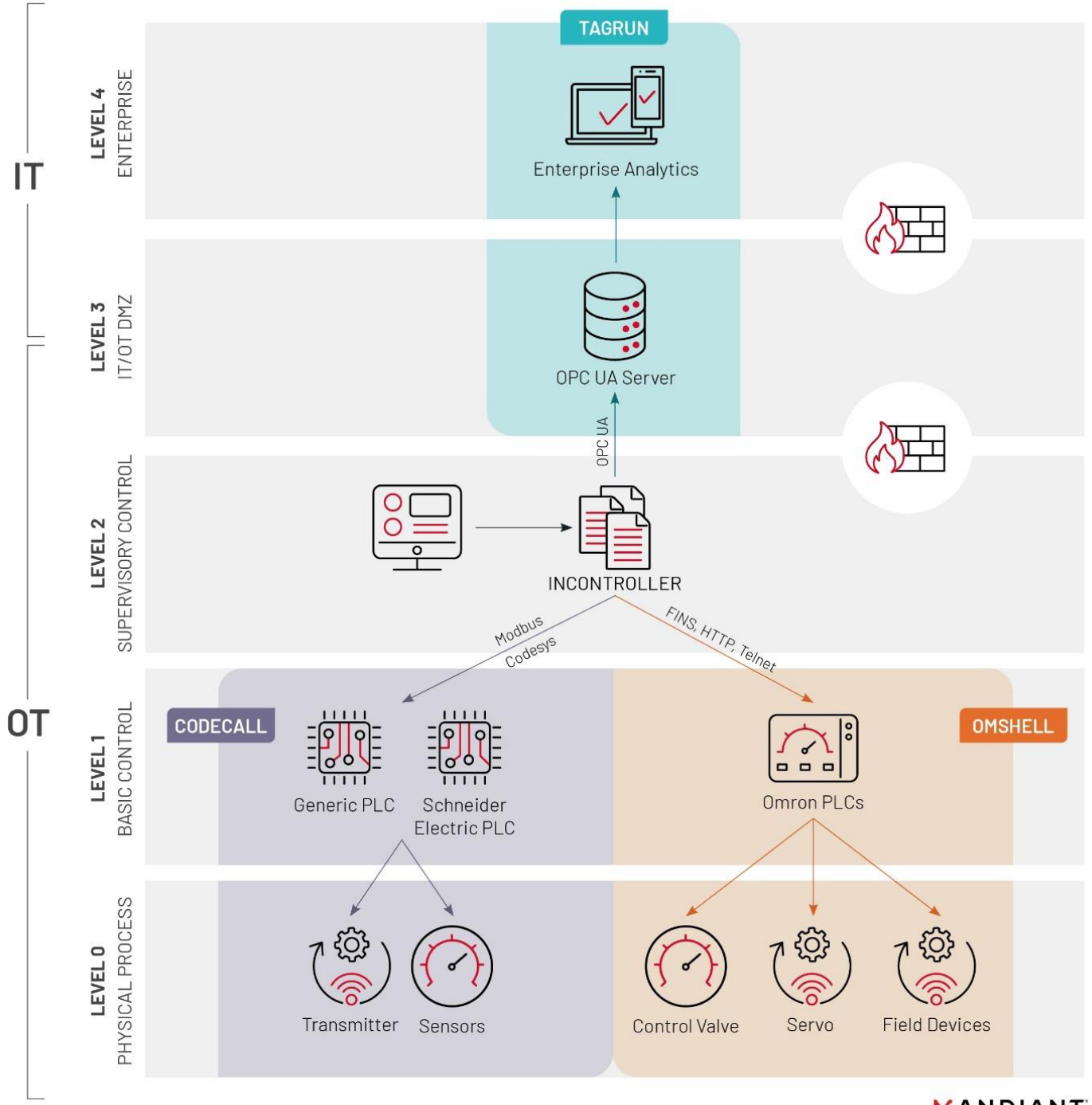
- Collection of three Python-based frameworks individually tracked as :
  - **TAGRUN**
  - **CODECALL**
  - **OMSHELL**
- They contain capabilities related to disruption, sabotage, and potentially physical destruction.
- Two additional tools affecting Windows-based systems that may be related to this threat activity include:
  - **ICECORE**
  - **An exploit for CVE-2020-15368**

Tool	Description
TAGRUN	A tool that utilizes an open-source OPC UA Python library to scan for OPC servers, enumerate OPC structure/tags, brute force credentials, and write OPC tag values.
CODECALL	A framework that communicates using Modbus—one of the most common industrial protocols. CODECALL contains modules to interact with, scan, and attack at least three Schneider Electric programmable logic controllers (PLCs).
OMSHELL	A framework with capabilities to interact with and scan some types of Omron PLCs. The tool can also interact with Omron's servo drives, which use feedback control to motors for precision motion control.

Note on attribution: *Currently unable to link to existing clusters of threat activity, but consistent with Russia's interest in ICS.*

- Limited initial indications, including a grammatical anomaly, suggest the malware was developed by Russian speakers
- Since at least 2014, Russia-nexus threat actors have targeted ICS assets and data with multiple ICS-tailored malware families (PEACEPIPE, BlackEnergy2, INDUSTROYER, TRITON, and VPNFILTER)

- Developed to allow the attacker to easily add new features to the malware over time
- Written in Python, possibly to leverage open-source projects to develop tool features, such as the OPC UA Python library



INCONTROLLER includes three tools that enable the attacker to send instructions to ICS devices using industrial network protocols, such as **OPC UA**; **Modbus**; **Codesys**, which is used by EcoStruxure Machine Expert and SoMachine; and **Omron FINS**.

While the tool's capabilities could enable the actor to communicate with a variety of products from different original equipment manufacturers (OEMs), the actor developed modules for specific controllers from Schneider Electric and Omron:

- **OPC servers**
- **Schneider Electric Modicon M251, Modicon M258, and Modicon M221 Nano PLCs**
  (Other devices leveraging Modbus and Codesys may also be affected)
- **Omron NX1P2 and NJ501 PLCs and R88D-1SN10F-ECT servo drive**
  (Other devices from NJ and NX PLC series may also be affected)

We highly doubt that the threat actor would target these devices at random. It is more likely they were chosen because of reconnaissance into specific target environment(s).

CODECALL

Modicon M221 Nano PLC

Modicon M258

Modicon M251

OMSHELL

NX1P2

NJ501

R88D-1SN10F-ECT

INDUSTROYER

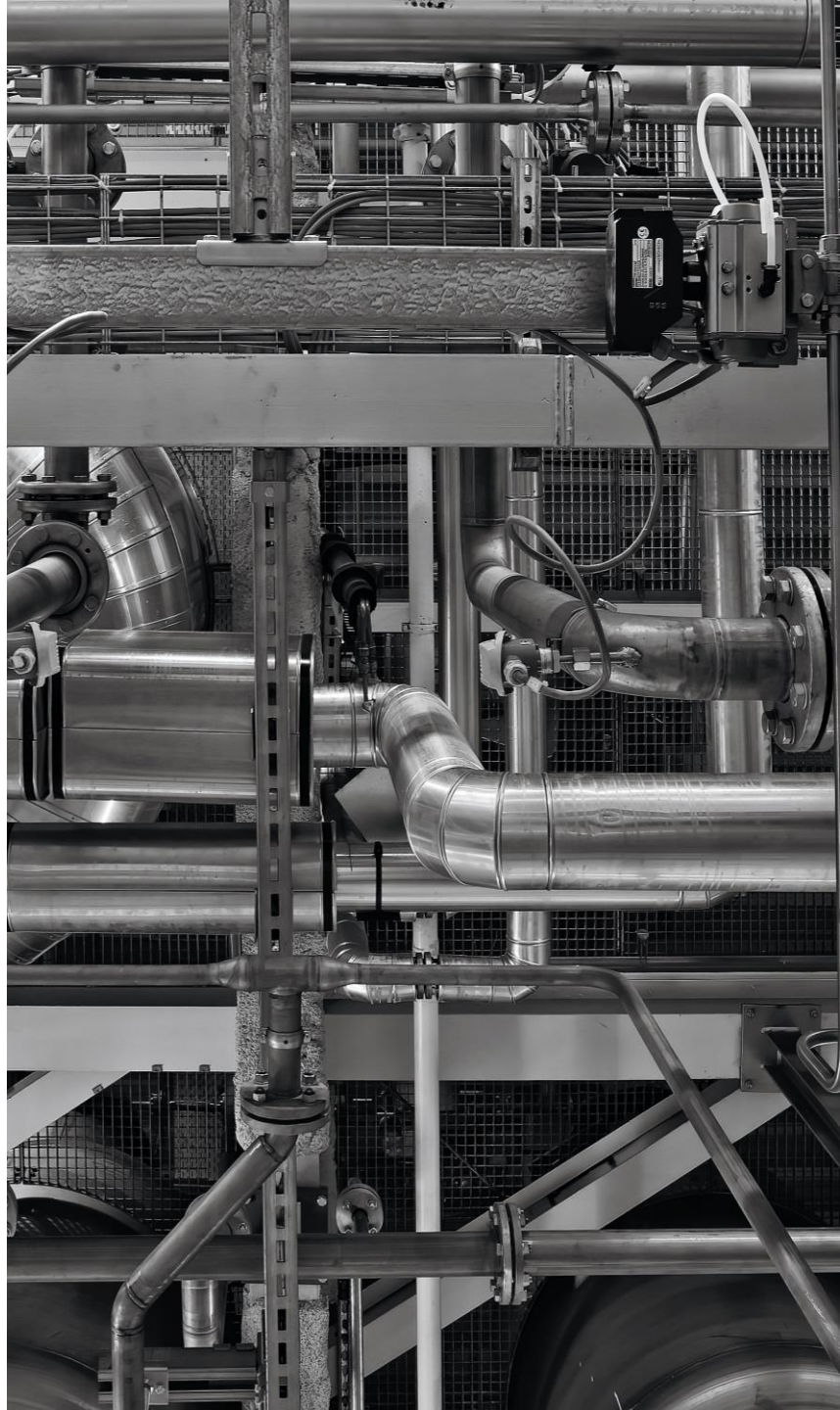
- **INDUSTROYER** is ICS-oriented malware with disruption capabilities that was previously leveraged to cause a power outage in Ukraine in December 2016
- **INDUSTROYER.V2** is similar to its predecessor, however, this variant contains more targeted functionality. Unlike the original INDUSTROYER, which was a framework that leveraged external modules to implement four different OT protocols, this variant is self-contained and only implements the IEC 60870-5-104 (IEC-104) communications protocol. IEC-104 is used for power system monitoring and control over TCP and is mainly implemented in Europe and the Middle.

The new malware variant enables the actor to embed customized configurations that modify the malware's behaviour to specific intelligent electronic devices (IEDs) (e.g., protection relays, merging units, etc.) within the target environment.

The design change to embed custom configurations in INDUSTROYER.V2 reduces the effort required by the actor to reproduce the attack against different victim environments and enables the actor to contain the impact to specific targeted IEDs.

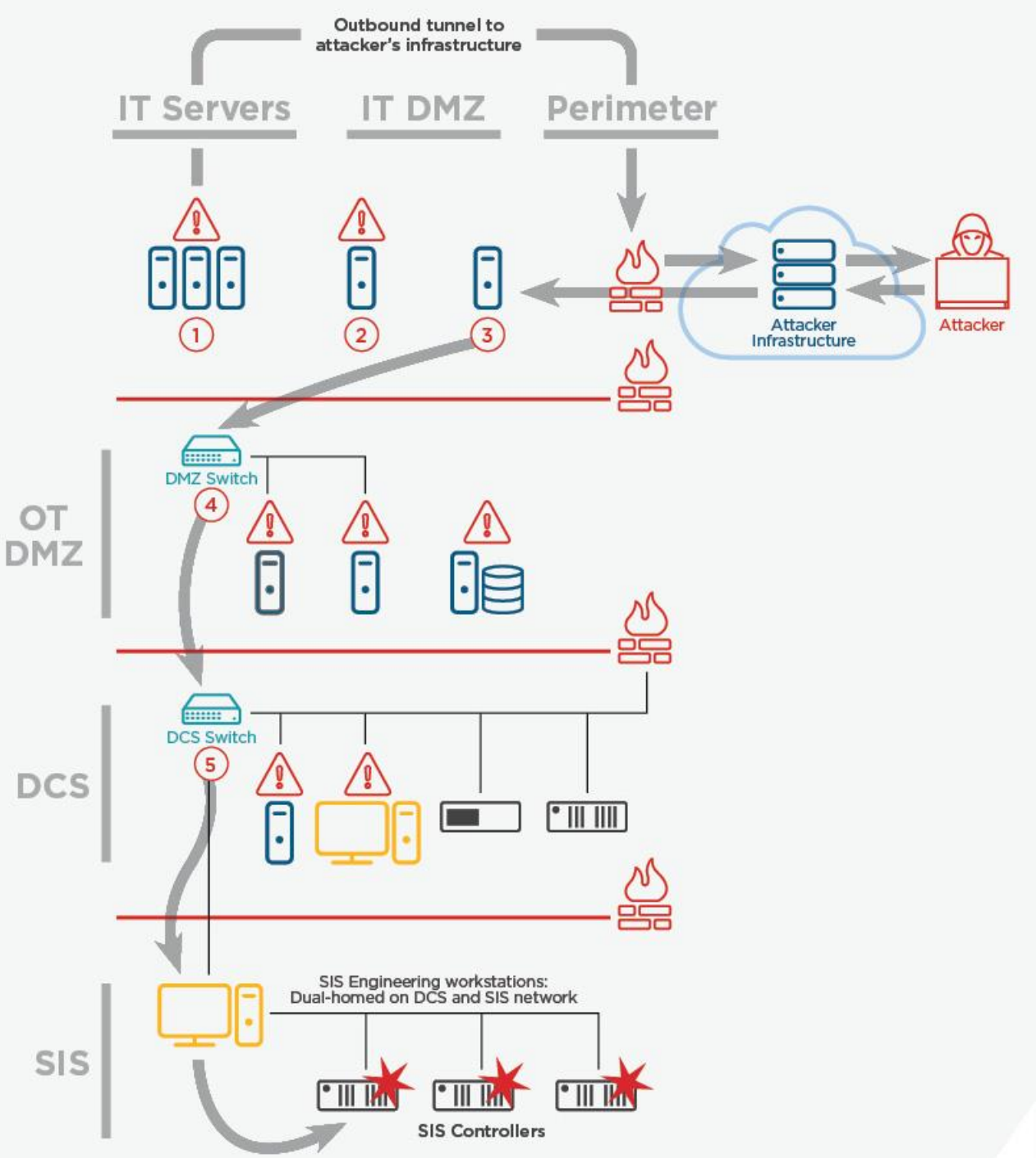
Tool	INDUSTROYER	INDUSTROYER.V2
Victim	Ukrainian transmission substation	Industrial control systems (ICS) supporting power grid operations in muiltiple substations in Ukraine
Protocols	IEC-101, IEC-104, IEC 61850, and OPC DA	IEC-104
Operation	Sending unauthorized command messages to open switches and circuit breakers via multiple ICS network protocols	Customized configurations that modify the malware's behaviour to specific intelligent electronic devices (IEDs)
Impact	Taking offline one-fifth of Kiev's power for 75 minutes (December 2016)	Possibly causing temporary outages to multiple electric substations (February – April 2022)

- While it is often believed that OT malware is not likely to be utilized in more than one environment, tools that take advantage of insecure by design OT features—such as INDUSTROYER.V2 does—can be employed multiple times to target multiple victims.
- The OT security community should recognize these tools as frameworks or capabilities and not merely features of isolated cyber security incidents.



- During the TRITON intrusion, the group appeared to be concentrated only on its core mission of obtaining access to and manipulating **Triconex SIS controllers**, ignoring unique opportunities to learn about the target industrial processes. They also practiced significant operational security to ensure they maintained prolonged and persistent access to the target environment.

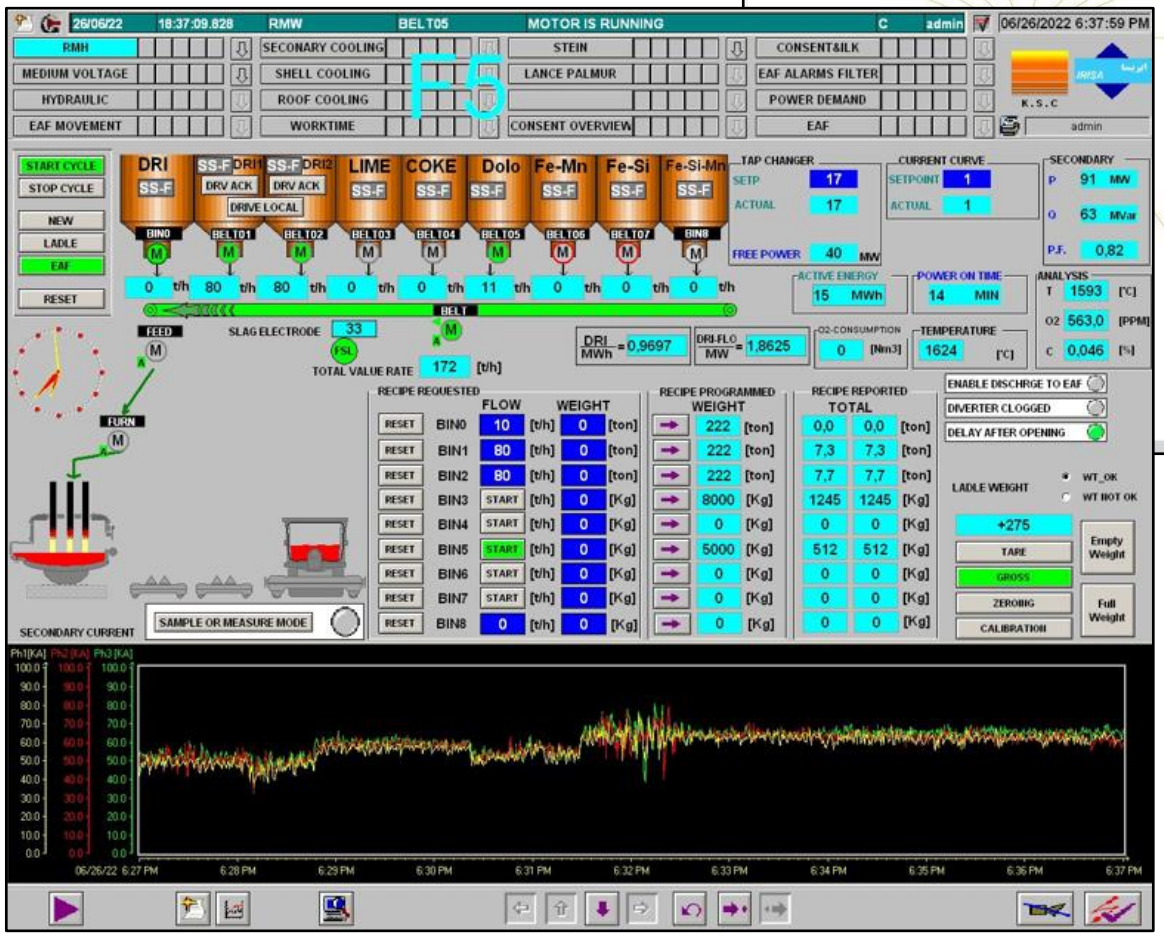
- The group ultimately reached the target SIS by compromising user accounts with VPN access to the distributed control system (DCS) network, and then targeting intermediary systems—networked workstations and servers using standard operating systems and protocols—as stepping-stones to gain access to the SIS. After obtaining privileged access to the SIS engineering workstation, attackers delivered the TRITON framework and attempted to inject a backdoor into the controller memory.



The Attack on Iran's Steel Plants

- On 27 June 2022, the cyber threat actor group dubbed "Predatory Sparrow" conducted an alleged disruptive and destructive cyber attack against three Iranian steel factories, forcing at least one of them to cease production operations, according to local and regional press.
- "Predatory Sparrow" likely jumped the air-gap between the networks through technical means, exploitation of misconfigured firewalls, or human enablement to gain access to the factory's HMI and manipulate the machinery.
- There are two likely possibilities for "Predatory Sparrow" to gain initial access to the steel factories:
  - First, in the video provided by "Predatory Sparrow" it shows Khuzestan Steel running an outdated PRTG monitoring software.
  - The other vector is a potential supply chain attack against Iranian engineering software firm **IRISA**, which is a joint investment with alleged victim Mobarakeh Steel Company. The three alleged victim steel manufactures are IRISA clients, which could explain why they were impacted by this attack.

Predatory Sparrow / Gonjeshke Darande



Predatory Sparrow / Gonjeshke Darande

Attack Element	Railway Attack (July 2021)	Fuel Stations Attack (Oct 2021)	Steel Attack (June 2022)
Malware Used	Destructive/Disruptive (Comet; Meteor; Stardust)	Unknown	Meteor Variant (without wiping functionality)
Assessed Level of Reconnaissance	High	High	High
Victim Industry	Transportation	Energy	Manufacturing
Critical Infrastructure	Yes	Yes	Yes
System Impacted	Electronic Train Tracking System	Online Fuel Management System	Steel Process Manufacturing Line
Messaging	Yes – "64411" and Supreme Leader Khamenei	Yes – "64411" and Supreme Leader Khamenei	Yes - "64411" and Supreme Leader Khamenei
Government Network Disrupted	Yes (Ministry of Roads and Urban Development)	Yes (NIOPDC)	None
Air-Gapped Network	Unknown	Yes (rumored)	Unknown

Hacktivism

- **במהלך החודשים האחרונים, אנו מזהים עליה בכמות האירועים למול תשתיות קריטיות, ארגונים תעשייתיים ומערכות OT/ICS מצד שחקנים מדינתיים. יחד עם זאת, בחודשים האחרונים, התעניינות דומה מזוהה גם בקרב קבוצות אחרות, אשר אינן פועלות בהכרח בחסות מדינתית (למשל, קבוצות האקטיביסטיות).**
  - **מוטיבציה** - בתור הסברים אפשריים למגמה, ניתן לציין את המלחמה באוקראינה ופעילות הסייבר ההתקפית של רוסיה בגזרה; ואת העלייה הגלובלית במחירי האנרגיה, המייצרת תחרות גדולה בשוק האנרגיה ואספקתה. דוגמא נוספת היא תקיפת הכופרה ב-Colonial Pipeline הממחישה גם את הפוטנציאל הכספי הרב שיש לאירוע סייבר המתרחש בסביבה תפעולית, או בסביבת IT הסמוכה לסביבת ה-OT.
  - **שינוי ב-TTPs** - במסגרת האירועים האחרונים, אנו מזהים שימוש בכלים פומביים, למשל במודולים ייעודיים של Metasploit למערכות OT/ICS, וזאת על ידי שחקנים ברמת תחכום נמוכה. מדובר בעדות לכניסתם של שחקנים חדשים לזירה אשר הייתה נשלטת עד כה על ידי שחקנים מדינתיים ברמה מקצועית גבוהה ביותר.

- **<u>ההקשר האזורי:</u>**
  - חקיינות והגברת החומות - תקיפת מפעלי הפלדה באיראן על ידי קבוצת Gonjeshke Darande יתכן ותשמש כטריגר לתגובת-נגד איראנית כנגד ישראל או בעלות בריתה (אשר חשודות במעורבות), יתכן במתווה דומה למול תשתית קריטית או תעשייתית.
  - קבוצות תקיפה שונות, אשר מרביתן מזוהות עם איראן, ממשיכות לטעון לאחריות על תקיפות DDoS ומבצעי Hack & Leak כנגד ישראל (מרבית הטענות אינן אומתו במלואן). אנו מעריכים כי פעילות זאת צפויה להימשך, וכמו כן גם הפעילות למול רכיבי ה-ICS, המתבצעת כעת בעיקר על ידי קבוצת GhostSec.
  - המתיחות סביב אסדות הגז והתגברות האיום הקינטי מצד חיזבאללה, יתכן ויובילו לפעילות נוספת כנגד ישראל במרחב הסייבר, זאת מצד חיזבאללה או מצד קבוצות אחרות הפועלות מלבנון תחת חסות איראנית.
  - צעדים נוספים בקידום הנורמליזציה בין ישראל למדינות האזור וההתפתחויות בשיחות הגרעין עם איראן, יתכן וישמשו כטריגר לפעילות סייבר כנגד ישראל.

יוני 2022

* - מידע לא מאומת

2 ביוני -
חברת **Microsoft** חשפה קמפיין תקיפה המכונה POLONIUM, הפועל מלבנון ותוקף יעדים בישראל (תשתיות קריטיות, תעשיה ביטחונית ו-IT)

2 ביוני -
קבוצה של גולים איראנים ("מוג'אהדין חלק") טוענת לתקיפת מצלמות אבטחה של המשטר באיראן ולהשחתת אתרים ממשלתיים

4-6 ביוני -
דיווחים תקשורתיים על מותם של שני מדענים איראנים בנסיבות לא ברורות; דיווח תקשורתי על מותו של בכיר ביחידה 840 של כוח קודס

7 ביוני -
קבוצת **JEA** טענה כי בצעה תקיפות על תשתיות אנרגיה וחשמל בישראל*; רומזת לאחריות על גרימה להפסקת חשמל באשקלון*

11 ביוני -
קבוצת **Altharea** טענה כי בצעה מתקפת DDoS נגד אתר הבורסה*

12-14 ביוני -
קבוצת **Sharp Boys** הדליפה מידע אישי רגיש ממספר אתרי תיירות ישראליים אשר נפרצו על ידי הקבוצה

14 ביוני -
חברת **Check Point** חשפה קמפיין פישינג איראני אשר הופנה כנגד בכירים לשעבר בישראל ובארה"ב (חשוד UNC788)

14 ביוני -
קבוצת **Mosses Staff** טענה כי תקפה את חברת החשמל, חברת "דוראד" וחברת מערכות הבקרה Realiteq*

20 ביוני -
שר הביטחון גנץ מצהיר כי ישראל בונה ברית הגנה אווירית אזורית בחסות אמריקאית

20 ביוני -
תקיפות סייבר, החשודות כאיראניות, על מערך האזעקות של מספר רשויות מקומיות (אילת וירושלים)

22 ביוני -
קבוצת **Mosses Staff** טענה לאחריות על התקיפה של מערכות האזעקה של הרשויות המקומיות (20 ביוני)*; טענה לפגיעה פיזית בבלון תצפית של צה"ל בגבול עזה*

23 ביוני -
דיווח על מעצר סוכנים איראנים בתורכיה אשר תכננו לפגוע בדיפלומטים ותיירים ישראלים

25 ביוני -
קבוצת Altharea טענה כי בצעה מתקפת DDoS על אתר משלוחי מזון ישראלי ("משלוחה")*

27 ביוני -
קבוצת **Gonjeshke Darande** טענה כי בצעה תקיפה על שלוש חברות לייצור פלדה באיראן, המזוהות לטענת הקבוצה עם משה"מ והבסיג'

28 ביוני -
קבוצת **GhostSec** הכריזה על השתתפות בקמפיין #OpIsrael, טענה כי בצעה תקיפה על מערכת בקרת קירור בישראל*

28 ביוני -
קבוצת **Sharp Boys** הדליפה מידע אישי רגיש מאתרי התיירות אשר תקפה בתחילת החודש; טענה לתקיפת אתרים נוספים*

קבוצות **1887 Team** ו-**Altharea** טענו כי ביצעו מתקפת DDoS על אתר חברת Cellebrite

29 ביוני -
ארגון **"חיזבאללה"** ניסה לשגר כלי טיס בלתי מאויש לעבר המים הכלכליים של ישראל

שר הביטחון גנץ האשים את איראן וארגון "חיזבאללה" בביצוע תקיפת סייבר כנגד יוניפי"ל; כמו כן, הצהיר כי יחידת סייבר של משה"מ בשם Shaid Kaveh פועלת על מנת להשיג מידע שמטרתו פגיעה בספינות, תחנות גז ומפעלים תעשייתיים

30 ביוני -
קבוצת **GhostSec** טענה כי בצעה תקיפות נוספות על מערכות בקרה (מים וחשמל) בישראל*

* - מידע לא מאומת

יולי 2022 (1)

2 ביולי -

ארגון "חיזבאללה" שיגר שלושה כלי טיס בלתי מאוישים לעבר אסדת הגז "כריש" (בפעם השנייה החודש)

2 ביולי -

קבוצת **GhostSec** טענה כי בצעה מתקפת DDoS על אתר חברת נת"ע (האחראית על פרויקט הרכבת הקלה והמטרו בגוש דן)

4 ביולי -

דיווחים תקשורתיים על מתקפת סייבר כנגד בנקים באיראן*

4 ביולי -

קבוצת **Altharea** טענה כי בצעה מתקפת DDoS על אתר חברת נת"ע (האחראית על פרויקט הרכבת הקלה והמטרו בגוש דן)

6 ביולי -

קבוצת **Sharp Boys** טענה כי תקפה 48 אתרים ישראלים, מרביתם פלטפורמות מסחר קטנות וחנויות טבע*

7 ביולי -

קבוצת **Gonjeshke Darande** הדליפה 20GB של מידע והתכתבויות דוא"ל שהושגו מתקיפת מפעלי הפלדה באיראן ב-27 ביוני (הדלפה ראשונה)

7 ביולי -

קבוצת **GhostSec** טענה כי בצעה תקיפות על מכשירי בקרה אלקטרוניים ומערכות בקרה תעשייתיות (ICS) בישראל*, ביניהם מערכת בקרת משאבות הביוב של עיריית אור עקיבא (זוהה בטעות על ידי התוקף כמערכת גז); קראה לפעילות משולבת כנגד אתרים של גופים ממשלתיים, חברות ממשלתיות ויעדים נוספים

9 ביולי -

קבוצת **GhostSec** טענה כי בצעה תקיפות נוספות על מערכות בקרה תעשייתיות בישראל*

9-10 ביולי -

בכירים איראניים ואתר Nour News, המזוהה עם המועצה העליונה לביטחון לאומי של איראן, הצהירו כי יצירת ברית ההגנה האזורית היא אקט "מאיים";

איראן הצהירה על התחלת העשרת האורניום ל-20% זאת באמצעות צנטריפוגות חדשות הנמצאת במתקן הגרעיני בפורדו

11 ביולי -

קבוצת **Altharea** טענה כי בצעה מתקפת DDoS על אתר עיריית תל אביב

12 ביולי -

קבוצת **GhostSec** דחתה פרסומים תקשורתיים אודות הטענות למעורבות הקבוצה ב"מלחמת הסייבר בין איראן לישראל"; טענה כי המוטיבציה מאחורי התקיפות היא סולידריות עם המאבק הפלסטיני

13 ביולי -

נסראללה נשא נאום במהלכו איים על ישראל, והצהיר כי כלי הטיס הבלתי מאוישים אשר נשלחו לעבר שדה הגז "כריש" היו "רק ההתחלה" וכי "יש הרבה יותר כבוד במלחמה מאשר המקום אליו הולכת לבנון כעת"

13 ביולי -

ביקור הנשיא ביידן בישראל

* - מידע לא מאומת

יולי 2022 (2)

14 ביולי -

הנשיא ביידן ורה"מ לפיד חתמו על "הצהרת ירושלים", המחייבת את שתי המדינות לעצירת איראן מהשגת נשק גרעיני, ומחייבת את ארה"ב לשמירה על העליונות הצבאית של ישראל;
טקס פתיחת משחקי המכביה

קבוצת **Gonjeshke Darande** הדליפה 10GB נוספים של מידע מתקיפת מפעלי הפלדה באיראן ב-27 ביוני (הדלפה שניה)

Cyberint מפרסמת דו"ח על קבוצת **GhostSec**

15 ביולי -

ביקור הנשיא ביידן בסעודיה - פסגת ג'דה בהשתתפות מנהיגי מדינות המפרץ לצד מנהיגי ירדן, מצרים ועיראק;

איחוד האמירויות מציינת כי לא תצטרף לברית האזורית נגד איראן

16 ביולי -

קבוצת האקרים אינדונזית טענה כי פרצה למספר אתרים ישראלים; חלק מהתארים הופיעו ברשימות אתרים שנפרצו בעבר*

קבוצת **Lab Doukhtegan** מדליפה את זהויותיהם של מספר האקרים איראנים המזוהים עם משה"מ

17 ביולי -

קבוצת **Altharea** טענה כי בצעה מתקפת DDoS על אתר משרד הבריאות, דבר שגרם למניעת הגישה לאתר מחו"ל (בצעד הגנתי)

קבוצת **GhostSec** רמזה כי פרצה לשרת אחסון אתרים ישראלי*

19 ביולי -

הנשיא פוטין צפוי לבקר באיראן, ולהיפגש עם מקבילו הנשיא ארדואן ונשיא איראן ראיסי; ישנם דיווחים גם על פגישתו המתוכננת עם המנהיג העליון ח'אמנהאי (פורום אסטנה)

19 ביולי -

קבוצת **Gonjeshke Darande** הדליפה 46GB נוספים של מידע מתקיפת מפעלי הפלדה באיראן ב-27 ביוני (הדלפה שלישית)

20 ביולי –

דיווחים על תקיפה טורקית בעיראק, במהלכה נהרגו אזרחים; טורקיה מכחישה את מעורבותה וטוענים כי מדובר באירוע טרור; בעקבות התקיפה קבוצות **Altahrea** ו-**1877** החלו בביצוע מתקפות DDoS נגד יעדים טורקים

22-24 ביולי -

קבוצת האקטיביסטים המזוהה עם ישראל (Army of Thieves) פורצת למספר אתרים של אוניברסיטאות באיראן ויעדים נוספים

24 ביולי –

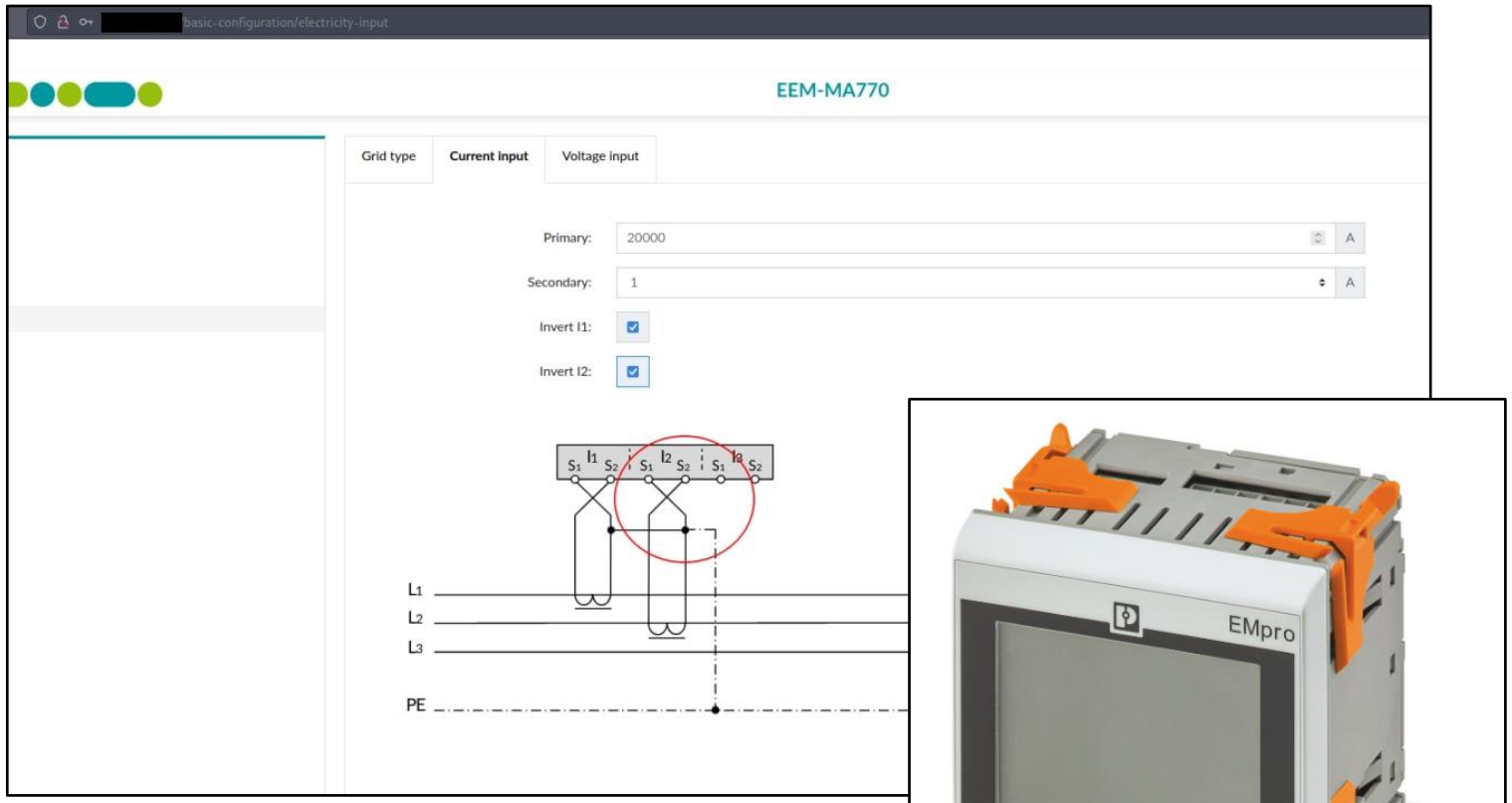
דיווח תקשורתי על מעצר שלושה אזרחים איראנים בטורקיה בחשד שתכננו להתנקש בישראלים, המעצר התבצע ב-14 ביולי;

דיווח תקשורתי לא מאומת על מות מסתורי של מהנדס טילים איראני נוסף

14 ביולי -

קבוצת **Altharea** טענה כי בצעה מתקפת DDoS על אתר עיריית ירושלים; מתקפת DDoS על אתר חברת 'רפאל'*;
כמו כן, טענה כי תקפה מערכת בקרה בתחנת הכוח "אורות יוסף" בנאות חובב, ורמזה לאחריות לשריפה אשר פרצה במקום;
הקבוצה טענה בהמשך כי תקפה מערכות בקרה נוספות בישראל

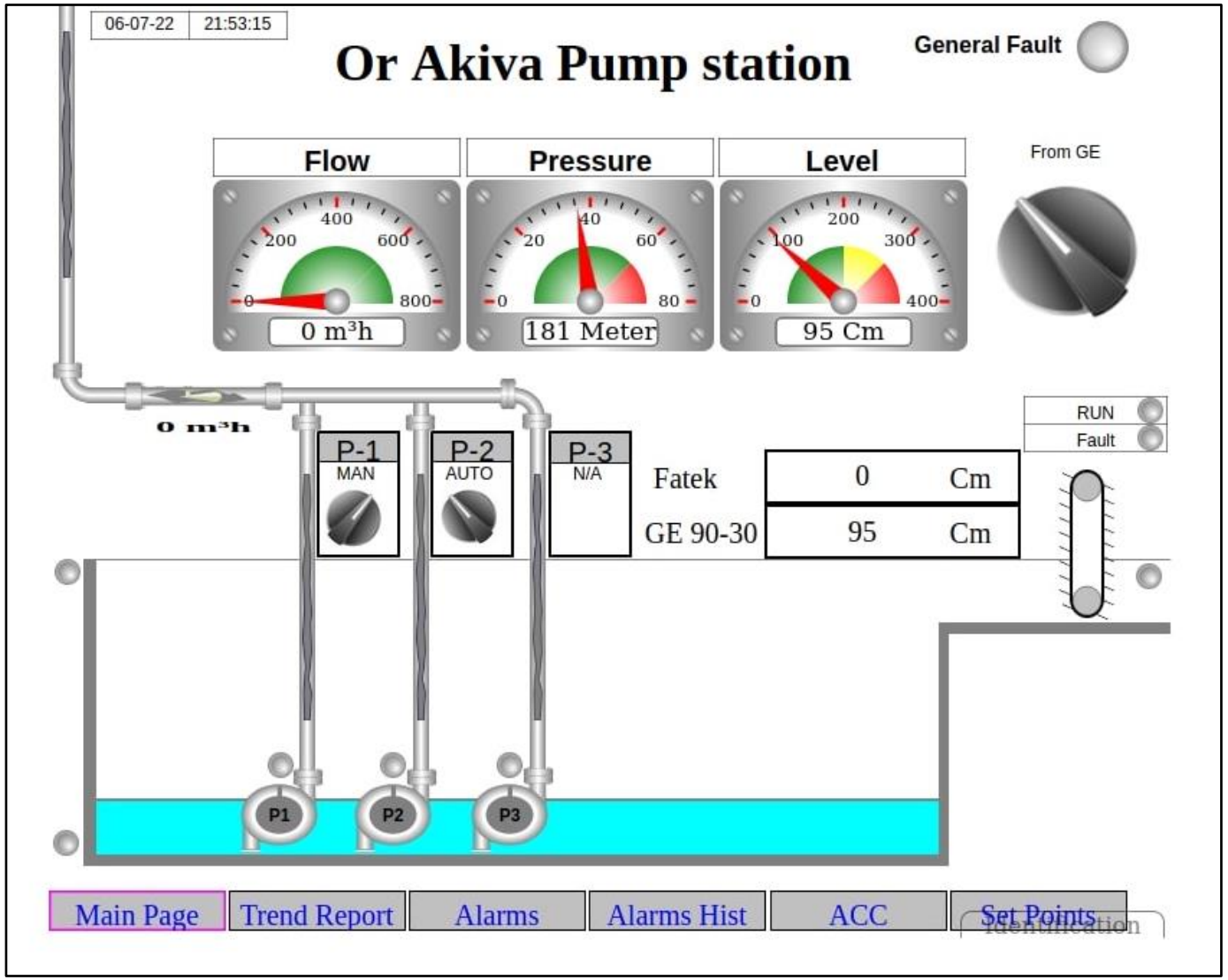
*מידע לא מאומת



EEM-MA770 / Phoenix Contact

ELNet

- Or Akiva's sewage pump control system interface compromised by 'GhostSec' group.
  - Ovarro TBox RTU / TWinSOft
  - Modbus client



Outlook

- Recently multiple hacktivist personas target or threaten certain internet-accessible ELNet industrial control system (ICS) assets in Israel. The targeted assets support energy metering processes and heating, ventilation, and air conditioning (HVAC) operations primarily for building automation environments.

- The targeted assets are affected by a vulnerability first reported in 2016 that allows the attackers to remotely manage the devices without authentication, which these threat actors could be exploiting in this activity.

- While we routinely observe hacktivists opportunistically target internet-accessible ICS assets, we rarely observe targeting overlaps and warn that these attacks can cause greater impacts at scale.

Vulnerabilities and Mitigation

Vulnerabilities Overview

- In the first quarter of 2022, CISA published 106 advisories related to vulnerabilities in ICS or medical devices.
  - The advisories presented information on 411 Common Vulnerability Enumeration (CVE) IDs, from which 85 (20%) received a Common Vulnerability Scoring System (CVSSv3) score of 9 or higher.
- In the first half of 2022, 681 ICS product vulnerabilities were disclosed.
  - Just over half of the 681 ICS vulnerabilities require a software patch, while 34% require a firmware update and 12% need a protocol update.
  - Approximately 13% of the 681 CVEs don't have a patch and may never get fixed — these are called "forever day vulnerabilities."

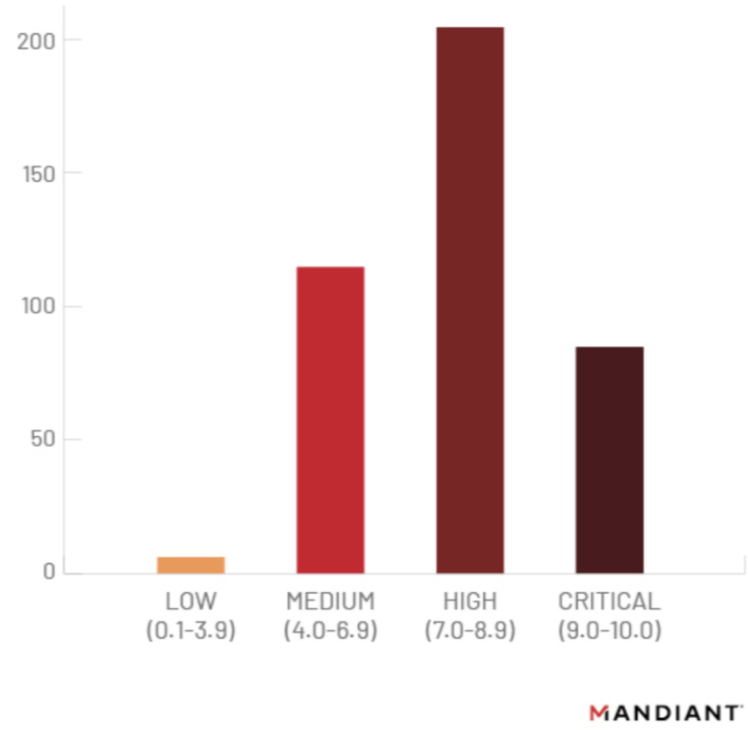


Figure 3: CVSSv3 score distribution for OT vulnerabilities reported by CISA between January – March 2022

- In 2021, we identified an upward trend in the number of disclosed vulnerabilities as ICS systems gain more interest from government, industry, and academia.
- The number of ICS and medical vulnerabilities disclosed in 2021 increased consistently with our observations from past years. The large number of vulnerabilities reported by Siemens highlight the value of conducting an internal CERT to facilitate and coordinate disclosure from researchers.
- As the volume of data that is released about ICS vulnerabilities increases, we expect to see more interest in understanding the trends and finding solutions to handle and categorize this information. This process could include, for example, translating ICS vulnerability information into popular markup languages or working on methodologies to assess risk to OT beyond the CVSS.

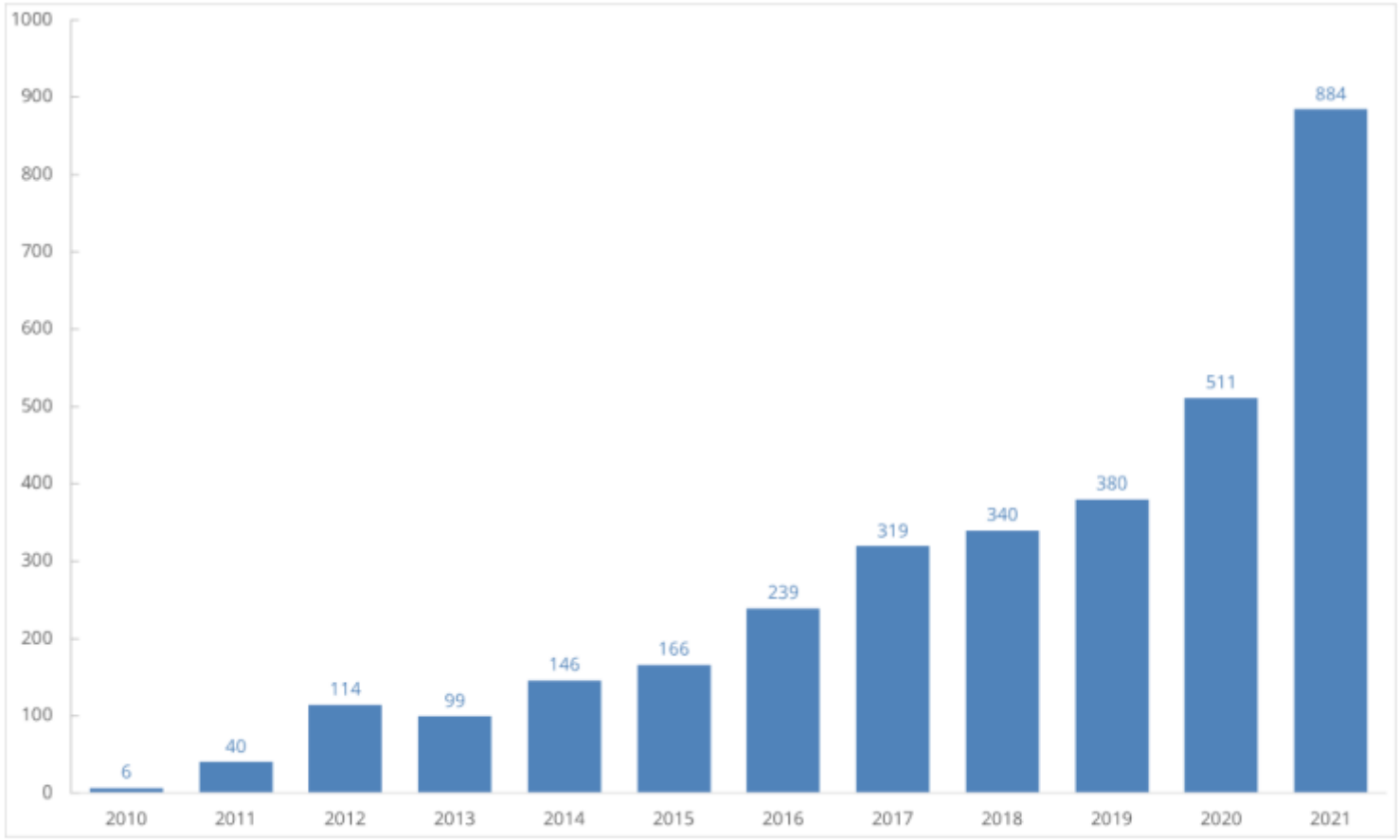


Figure 1: CISA yearly disclosed vulnerabilities between March 2010 and December 2021

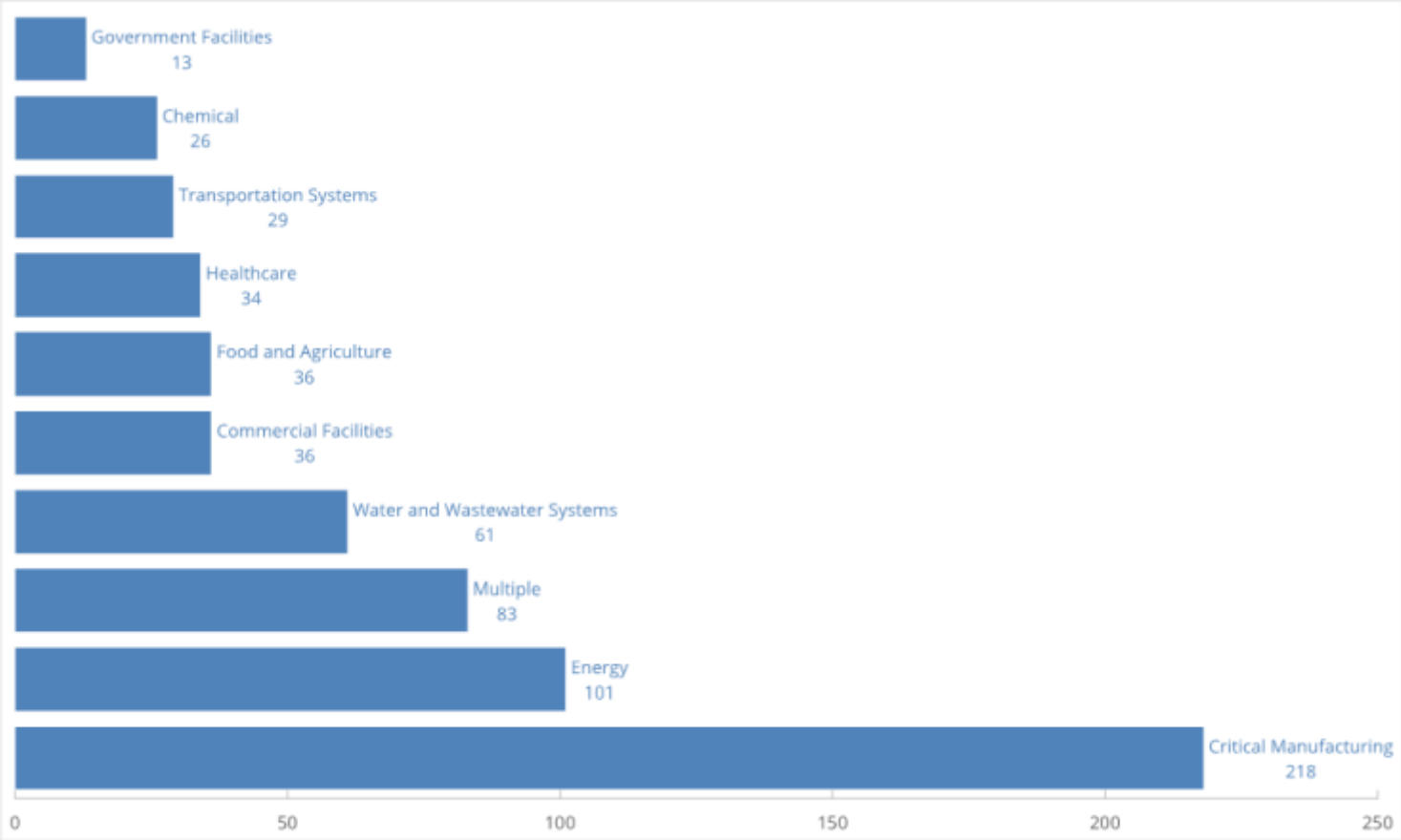


Figure 2: Top 10 affected industries by sector

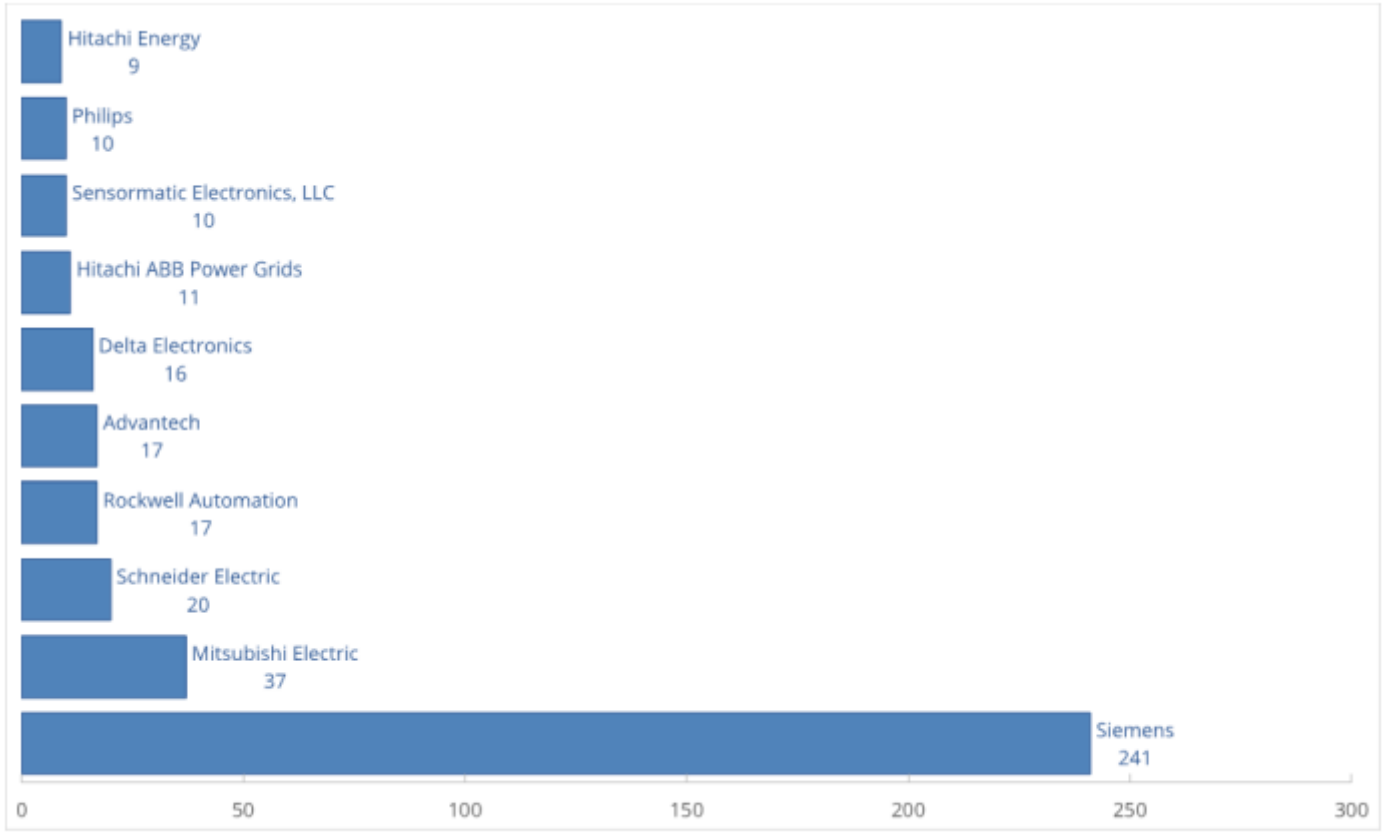


Figure 3: Top 10 vendors for all 2021 CISA advisories

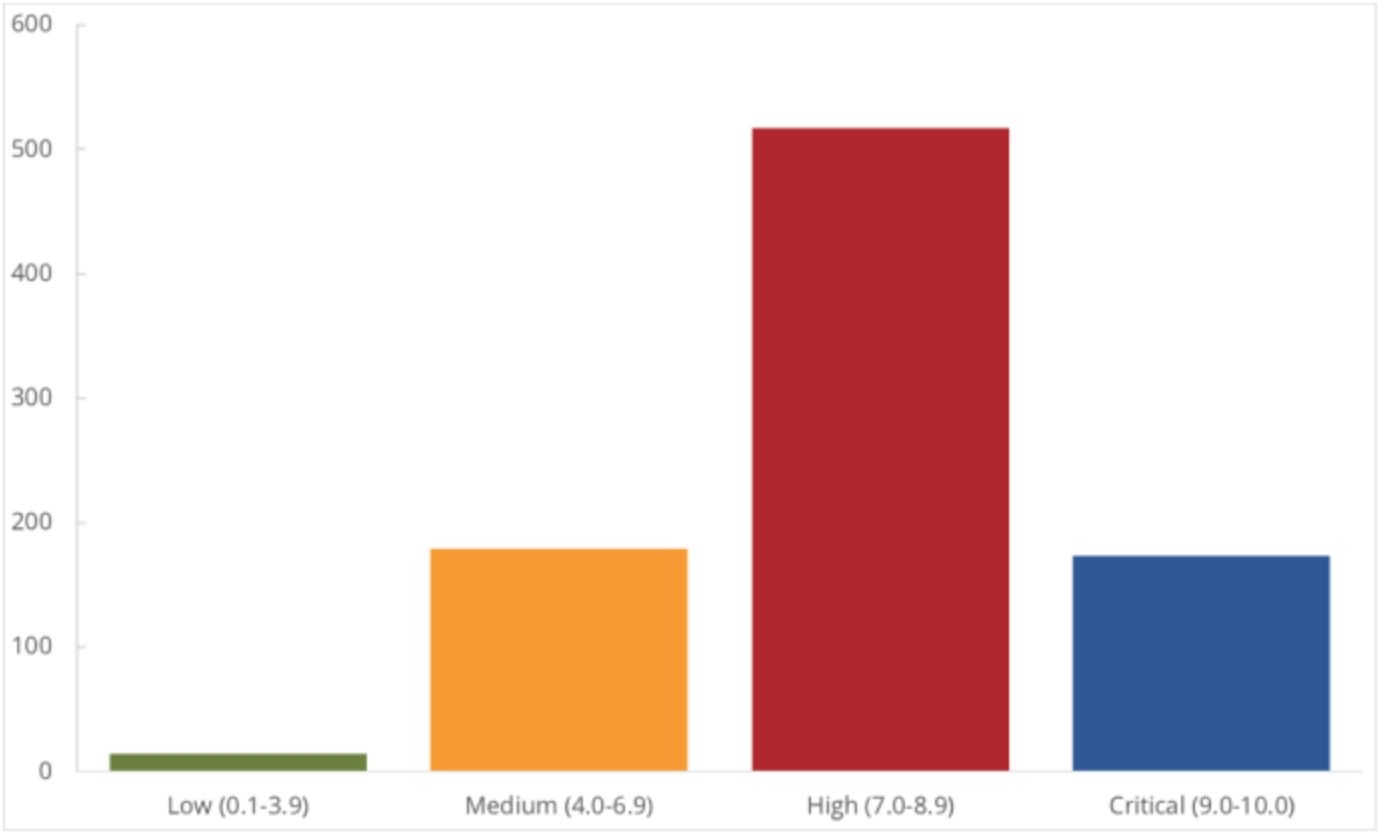
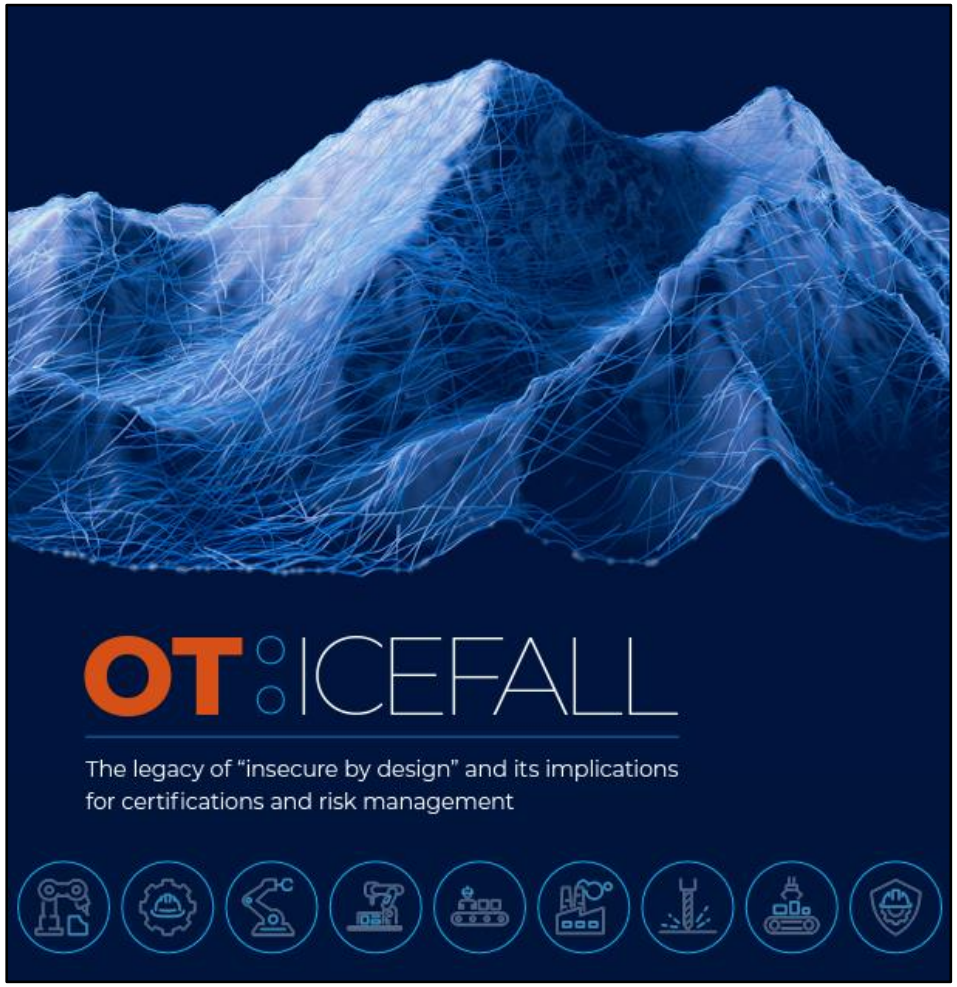


Figure 4: Vulnerabilities by severity



Forescout discloses **OT:ICEFALL**; 56 vulnerabilities impact ten vendors, including: Bently Nevada, Emerson, Honeywell, JTEKT, Motorola, Omron, Phoenix Contact, Siemens, and Yokogawa.

Commonly existing PLC Supply Chain Threats: Multiple critical vulnerabilities in Codesys Runtime

Abstract

- We conducted an in-depth research on CODESYS V2 runtime and PLCs using this kernel (ABB AC500 PLCs)
- We found 11 vulnerabilities in CODESYS V2 runtime;
- 2 of all accepted vulnerabilities graded as critical, 7 as high risk, and 2 as medium risk.
- These vulnerabilities are simple to exploit, and they can be successfully exploited to cause consequences such as sensitive information leakage, PLCs entering a severe fault state, and arbitrary code execution. In combination with industrial scenarios on field, these vulnerabilities could expose industrial production to stagnation, equipment damage, etc.
- CodeSys has published an official security advisory that has fixed the mentioned vulnerabilities. However, many vendors who use CODESYS V2 runtime have not yet updated in time, in which case factories using these affected products are still in serious risk.
- The manufacturers who use CODESYS V2 runtime include, but not limited to, ABB, WAGO, IFM, EPEC, Beckhoff, Kontron, Moeller, Festo, several Russian industrial control manufacturers, and several Chinese industrial control manufacturers.

Recommendations

- Proper segmentation of information technology (IT) and operational technology (OT) networks aids in preventing attackers pivoting from corporate networks into industrial environments.
- Whitelisting accepted master/slave devices, behavior patterns, and commands aids in establishing approved baselines and detecting anomalies with the aid of network monitoring.
- Implementation of an industrial firewall with deep packet inspection aids in controlling access and approved capabilities.
- Implementation of ICS-aware intrusion protection systems aids in monitoring for function codes from potentially malicious sources.
- Enable security feature, such as authentication and encryption, especially for critical assets, where support for these features exists.

Q&A

MANDIANT®

YOUR CYBERSECURITY ADVANTAGE

Thank You

German Simkin
0547906908
german.simkin@mandiant.com


MANDIANT®
YOUR CYBERSECURITY ADVANTAGE