

# Analysis of and Mitigation Strategies for Real World ICS Security Incidents



**Fraunhofer**  
AISEC



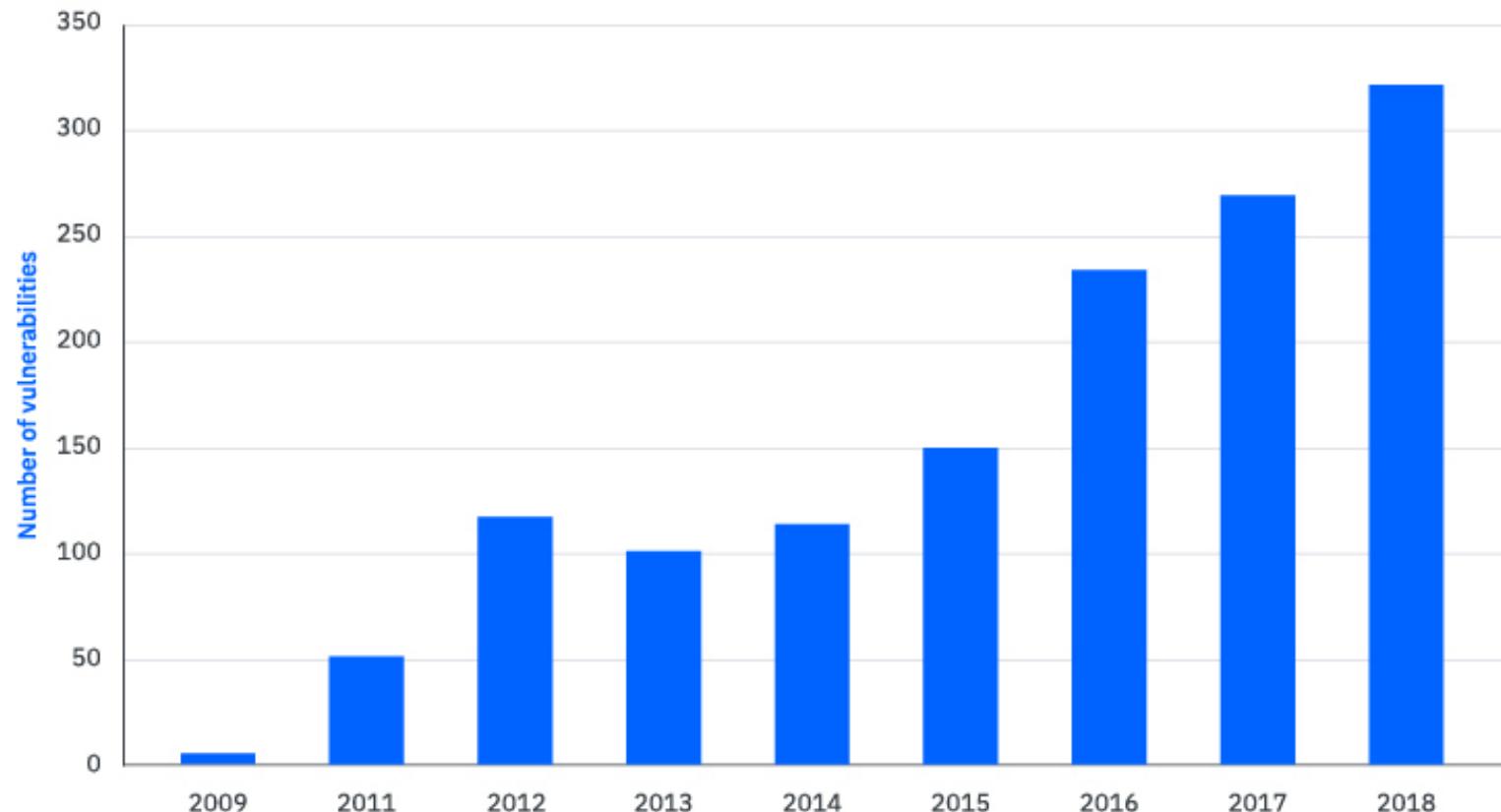
Nico Fechtner

*nico.fechtner@tum.de*

June 4, 2020

# Growing ICS Threat Landscape

**X-Force Red Vulnerability Database Total ICS Vulnerabilities**



# Problem Statement

Defend against ICS attacks



Avoid known/common mistakes



Learn from past incidents



**Comparative overview of historic incidents**

+

**In-depth analyses of individual incidents**

# Agenda

- Motivation & Problem Statement
- Comparative Overview of ICS Security Incidents
- Case Study: The Triton Attack
- Conclusion & Future Work

# Agenda

- Motivation & Problem Statement
- Comparative Overview of ICS Security Incidents
- Case Study: The Triton Attack
- Conclusion & Future Work

## Analyzed Incidents

Incident enumerations (Risi database, ICS-CERT alerts)

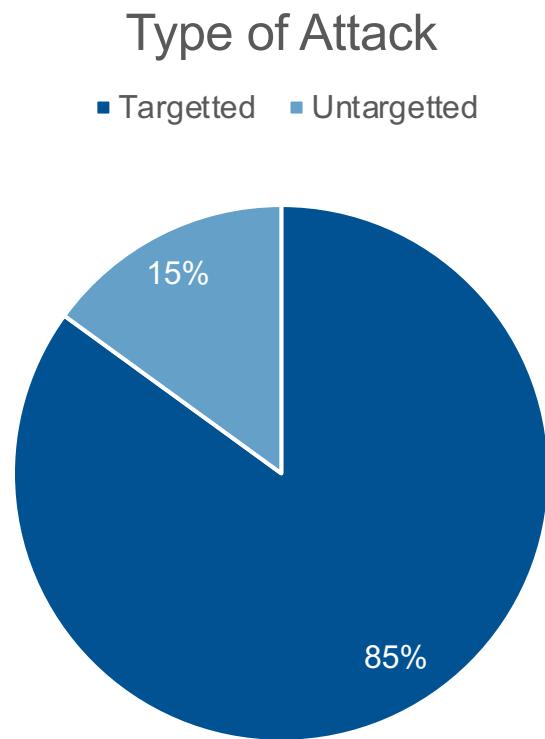
Threat reports from ICS security companies

Papers / conference talks dedicated to single incidents

Press releases / blog posts dedicated to single incidents

27 incidents analyzed

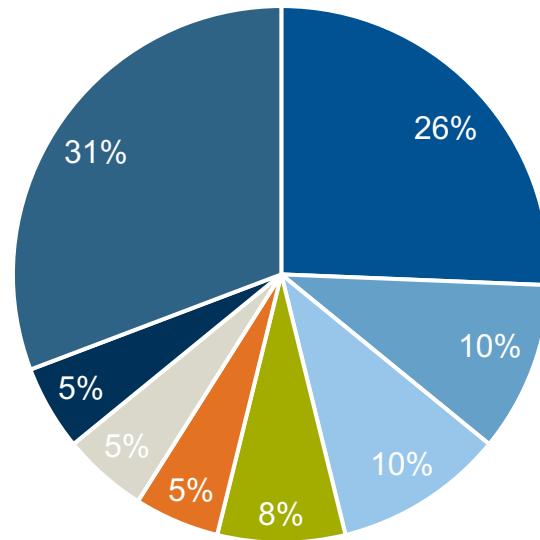
## Targets



## Targets

### Targeted Sectors

- Energy
- Manufacturing
- (Petro)chemical
- (Waste)water
- Technology
- Government
- Aviation
- Other



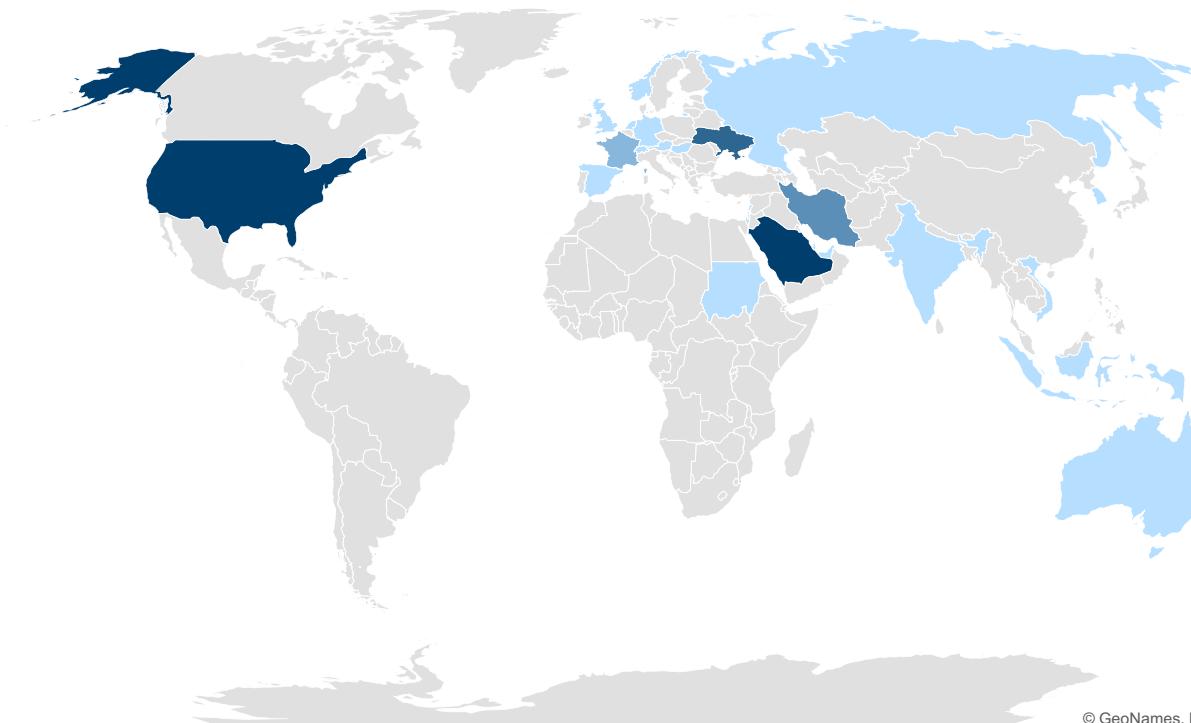
## Targets

Targeted Regions

# Incidents



1                    5



Powered by Bing  
© GeoNames, Microsoft, Navinfo, TomTom, Wikipedia

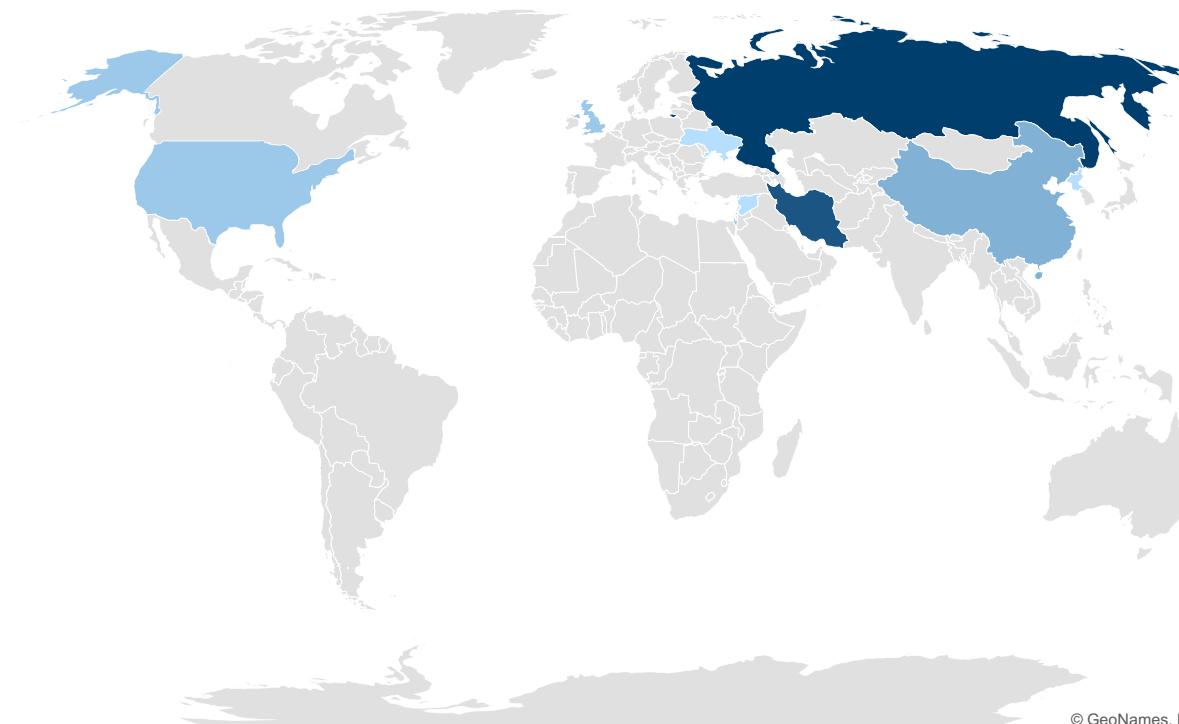
## Threat Actors

Home Countries of Threat Actors

# Incidents

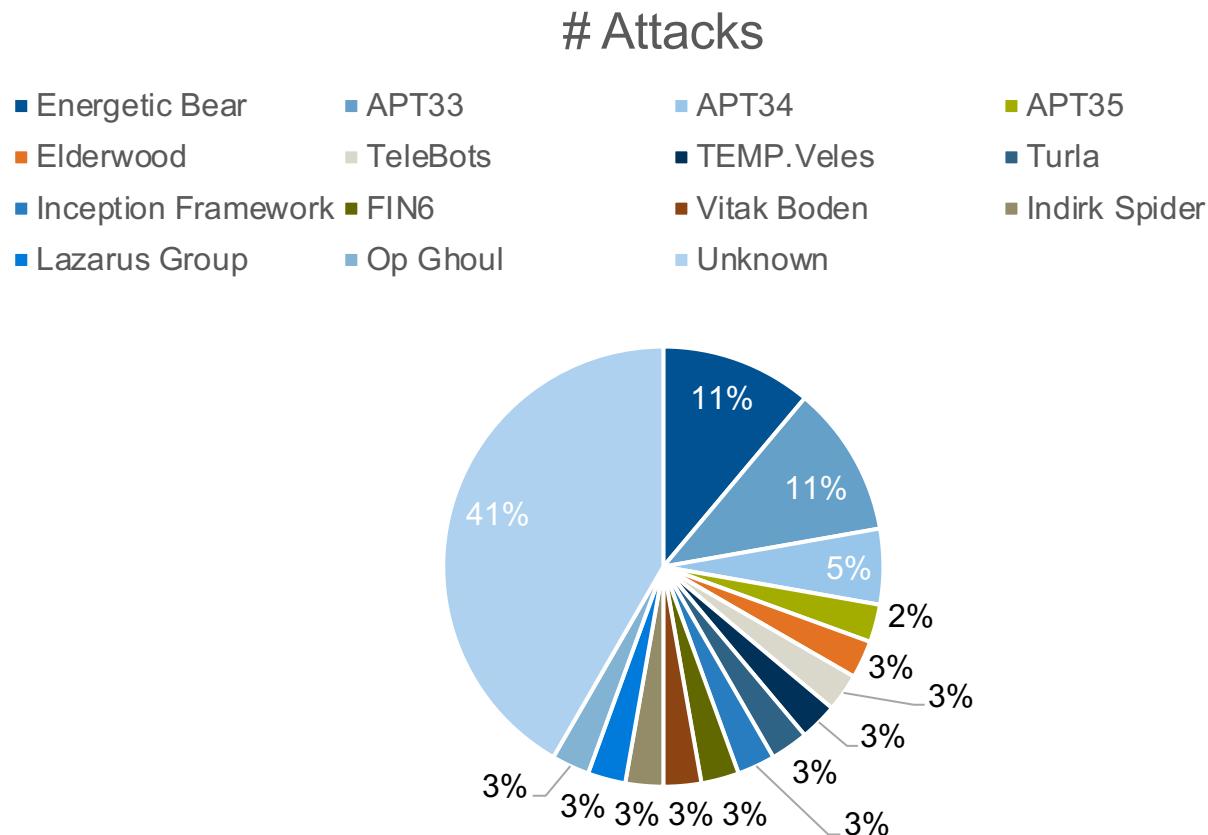


1                    8



Powered by Bing  
© GeoNames, Microsoft, Navinfo, TomTom, Wikipedia

## Threat Actors



## Attack Techniques

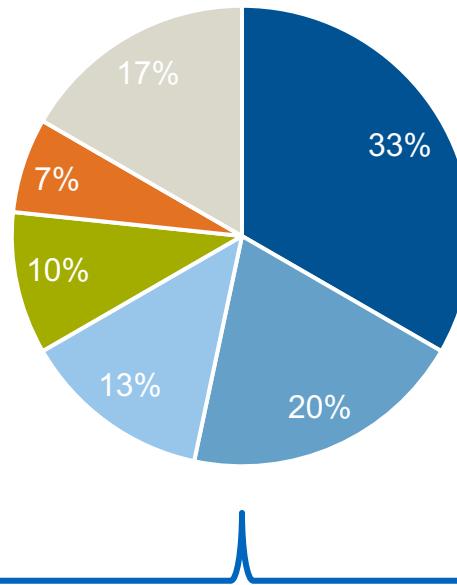
**Exploit Windows Vulnerabilities**

Mimikatz Living Off The Land Tools  
Ransomware Malware SIS Tampering  
Wipe HMs Obfuscation  
Spearphishing Cobalt Strike  
RDP Brute Force PsExec  
PowerShell Wiperware 0-Day Exploits  
Digital Signatures Social Engineering  
Scalable ICS Attack Frameworks  
Exploit AAD Vulnerabilities  
Malware Evasion Metasploit  
EternalBlue

## Attack Goals and Motivations

Attack Goals

- Steal data
- Cause disruption
- Ransom payment
- Cause physical damage
- Financial gain via data selling
- Other

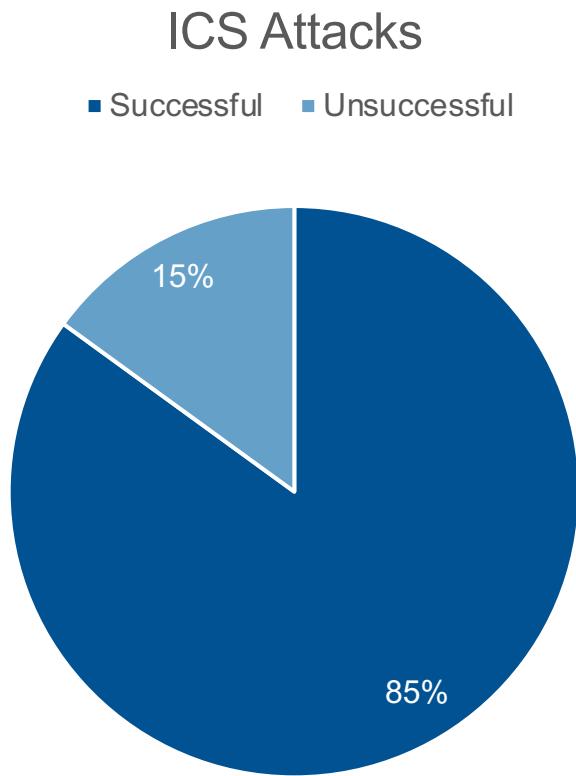


Monetary Gain

Information Gain

(Physical) Disruption

## Success Rate



## Dwell Times

- Dwell Time of untargetted attacks: Days
- Dwell Time of targetted attacks: Months – Years



- In theory a lot of time to detect and prevent the execution of a payload
- In practice most attacks still are not detected in their early stages

## Detection and Mitigation Strategies

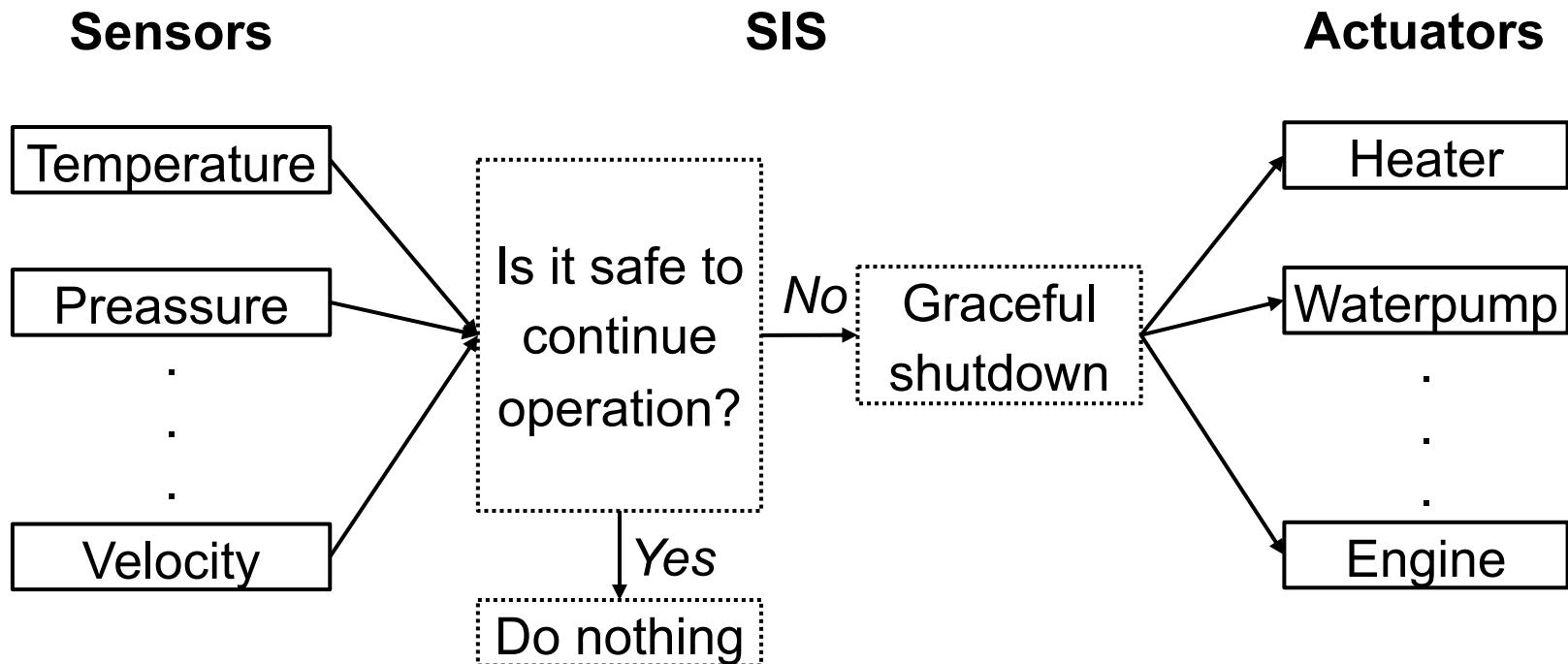
- Up-to-date asset inventory
- Intrusion detection/prevention systems (IDS)
- Increasing the security awareness of employees
- Vulnerability management solutions
- Solid backup strategy

# Agenda

- Motivation & Problem Statement
- Comparative Overview of ICS Security Incidents
- Case Study: The Triton Attack
- Conclusion & Future Work

# Safety Instrumented Systems (SIS)

**Goal:** Maintain safe operations and prevent catastrophic events in case of failures of other hard- or software.



## Attack and Response Strategies

- Still unclear how the ICS network got breached; possibly through spearphishing



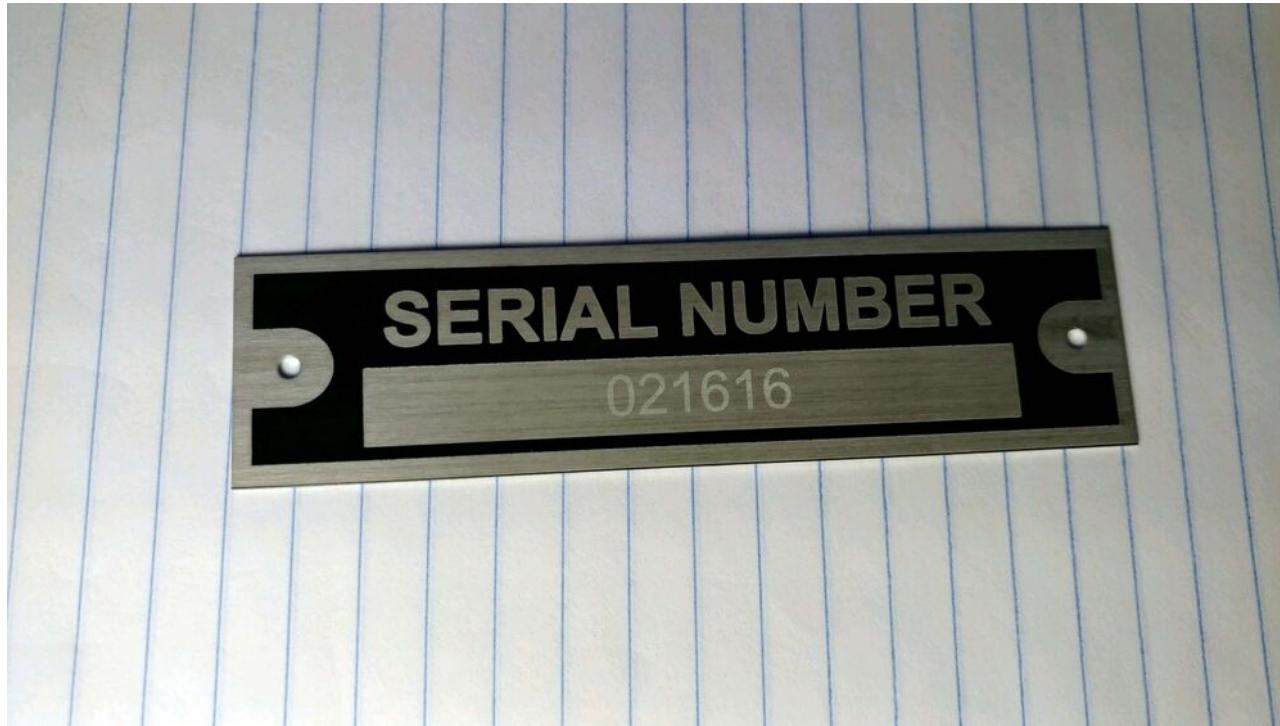
## Attack and Response Strategies

- Since the network connectivity of the SIS was not strictly limited, the attackers could access it



## Attack and Response Strategies

- Attackers figured out the exact SIS model and left for two years



## Attack and Response Strategies

- After returning, they installed the Triton malware on the SIS



## Attack and Response Strategies

- After installation and execution, the plant tripped gracefully



## Attack and Response Strategies

- Due to a programming error the malware contained a bug



## Attack and Response Strategies

- After some investigations, the plant was brought up again



## Attack and Response Strategies

- The attackers got a second chance, tried to fix the bug and installed Triton again



## Attack and Response Strategies

- Due to the bug not being patched correctly the plant tripped again



## Attack and Response Strategies

- Hired ICS security specialists were able to identify and remove the malware



## Goals, Impacts, and Attribution

- Goal: remains unclear; probably to cause disruption
- Impact: Several weeks of downtime
- Attribution: State-sponsored Russian threat group named TEMP.Veles

## Detection and Mitigation Opportunities

- **Continuous security awareness trainings** can help employees to identify phishing attacks
- **Restricting the network connectivity of a SIS** lowers the possibility of a SIS breach
- Under normal circumstances, **SIS should always operate in *run* mode**, not in *program* mode in order to prevent reprogramming of the logic by attackers

# Agenda

- Motivation & Problem Statement
- Comparative Overview of ICS Security Incidents
- Case Study: The Triton Attack
- Conclusion & Future Work

# Conclusion

- Untargetted attacks are becoming increasingly important
- Most attacks are considered to be state-sponsored
- Important trends in terms of attack techniques are spearphishing, zero-day exploits, sophisticated obfuscation and evasion techniques, and living off the land tools
- The most common goals of ICS attacks are data extraction and causing disruption
- Attackers usually reside in the victims' network for several weeks or months before executing the final payload

# Conclusion

- Up-to-date asset inventories
- Intrusion detection/prevention systems (IDS)
- Increasing the security awareness of employees
- Vulnerability management solutions
- Solid backup strategies

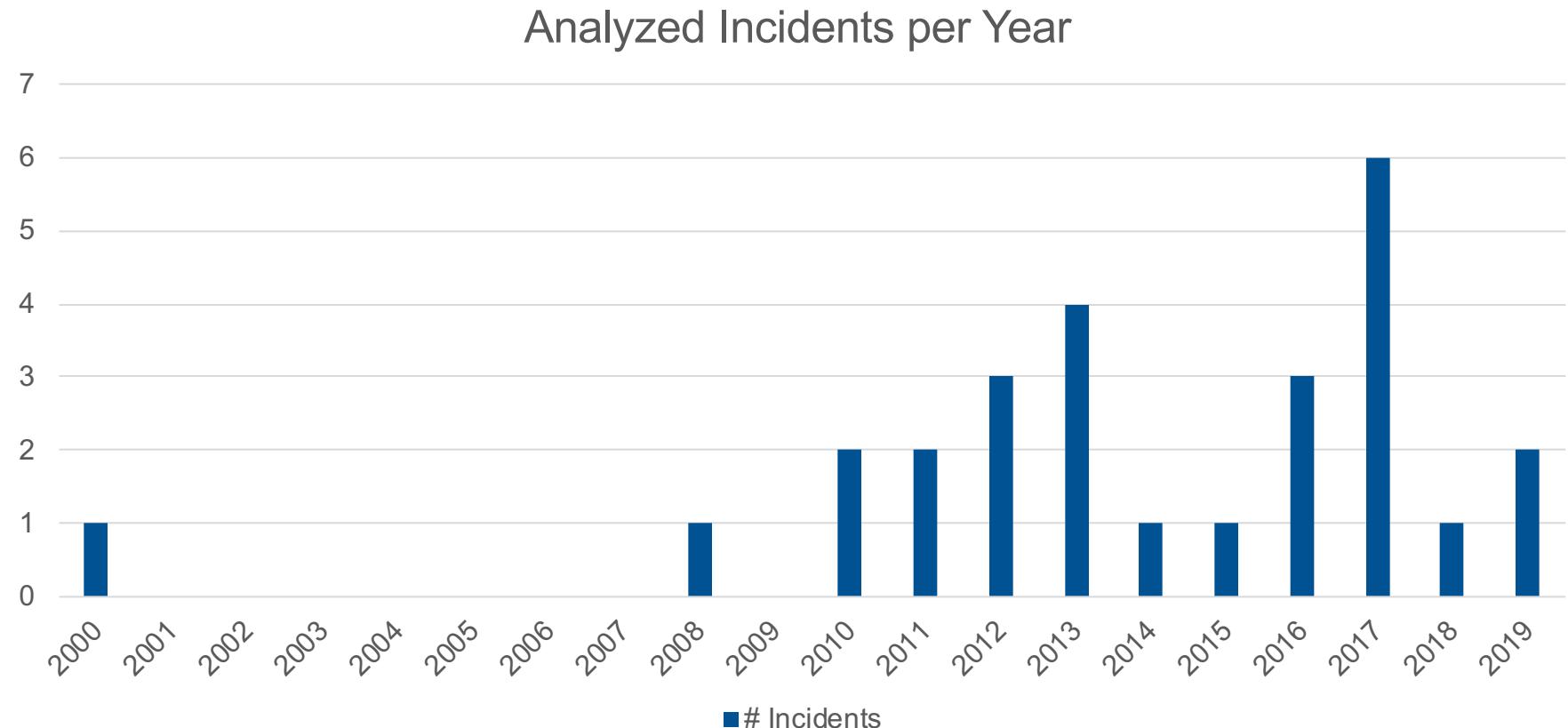
# Future Work

- Add more incidents for higher accuracy and deeper insights
- Use an analysis approach that is more qualitative instead of quantitative
- Analyze how ICS companies manage to defend against known threats over the course of time

# Q & A

# Backup

## Analyzed Incidents



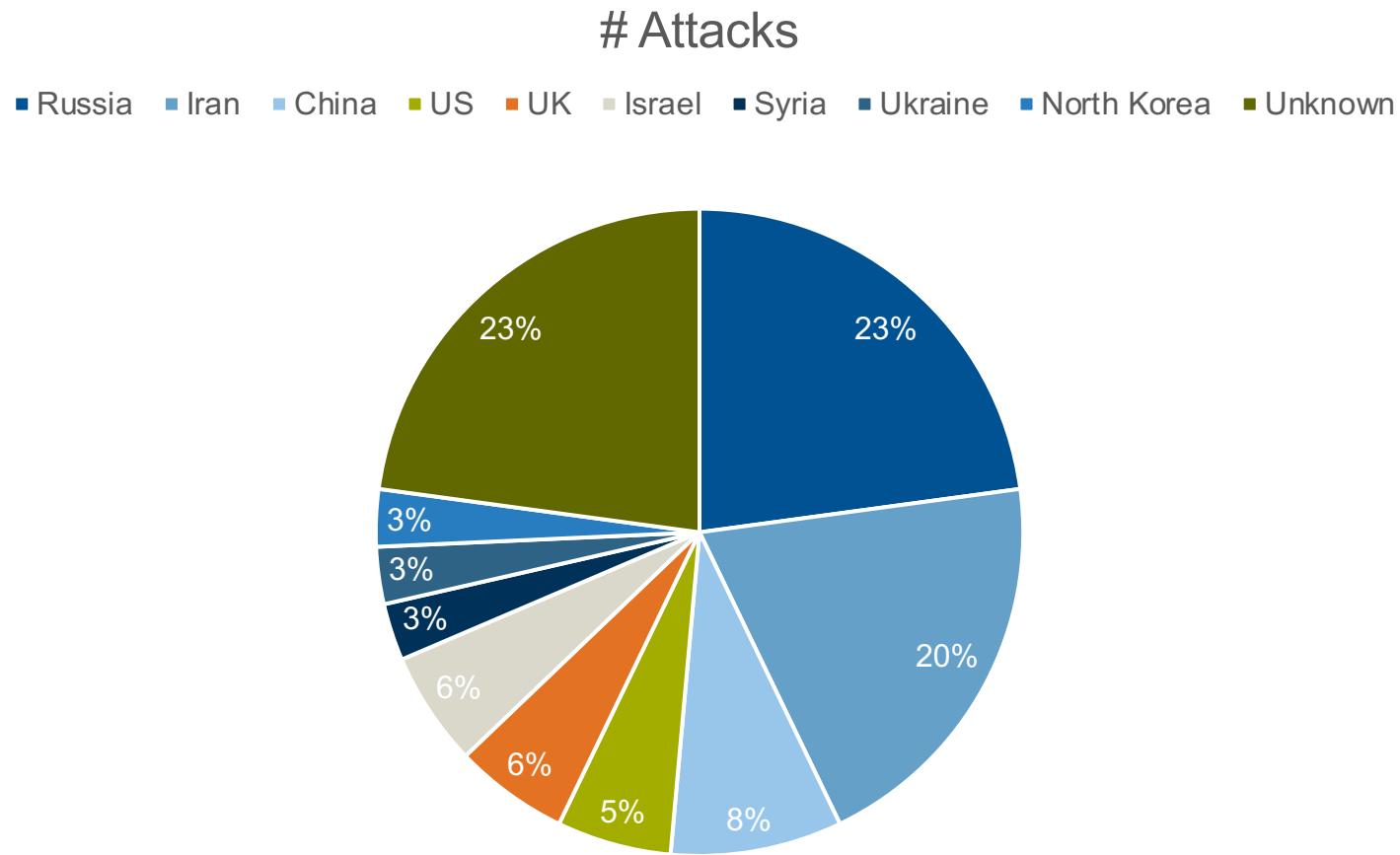
# Comparative Overview of ICS Security Incidents

- Targets
- Threat actors
- Attack techniques
- Attack goals and realized impacts
- Dwell times and reactions
- Detection and mitigation strategies

# Analyzed Incidents

Incident	Impact	Targeted	Region	Sector
Maroochy Water	2000	Yes	Australia	(Waste)water
Conficker	2008	No	Multiple	Multiple
Stuxnet	2010	Yes	Iran	Nuclear Power
NightDragon	2010	Yes	Global	Multiple
Duqu	2011	Yes	Multiple	Multiple
Gas Pipeline Intrusion Campaign	2011	Yes	Unknown	Energy
Shamoon	2012	Yes	Middle East	Energy
Flame/sKyWIper	2012	No	Middle East	Unknown
Gauss	2012	Yes	Middle East	Unknown
Red October	2013	Yes	Multiple	Gov / Research
Target Store's HVAC	2013	Yes	US	Retail
New York Dam	2013	Yes	US	Water
Havex/Backdoor.Oldrea	2013	Yes	US/Europe	Multiple
German Steel Mill	2014	Yes	Germany	Manufacturing
BlackEnergy(3)	2015	Yes	Ukraine	Energy
Industroyer/CRASHOVERRIDE	2016	Yes	Ukraine	Energy
Kemuri water company	2016	Yes	US	Water
Op Ghoul	2016	Yes	Multiple	Multiple
WannaCry	2017	No	Multiple	Multiple
NotPetya	2017	Yes	Ukraine	Multiple
BitPaymer	2017	Yes	Multiple	Multiple
Dragonfly 2.0	2017	Yes	Unknown	Energy
Triton/Trisis/Hatman	2017	Yes	Saudi Arabia	Chemical
StoneDrill	2017	Yes	Saudi Arabia	Unknown
Shamoon 3	2018	Yes	Multiple	Multiple
LockerGoga	2019	Yes	Multiple	Multiple
Maze/ChaCha	2019	No	Multiple	Multiple

## Threat Actors



# Attack and Response Strategies

- Unclear how the ICS network got breached; possibly through spearphishing
- Since the network connectivity of the SIS was not strictly limited, the attackers could access it
- Attackers figured out the exact SIS model and left for two years
- After returning, they installed the Triton malware on the SIS

# Attack and Response Strategies

- After installation and execution, the plant tripped gracefully
- Due to a programming error the malware contained a bug
- After some investigations, the plant was brought up again
- The attackers got a second chance, tried to fix the bug and installed Triton again
- Due to the bug not being patched correctly the plant tripped again
- Hired ICS security specialists were able to identify and remove the malware