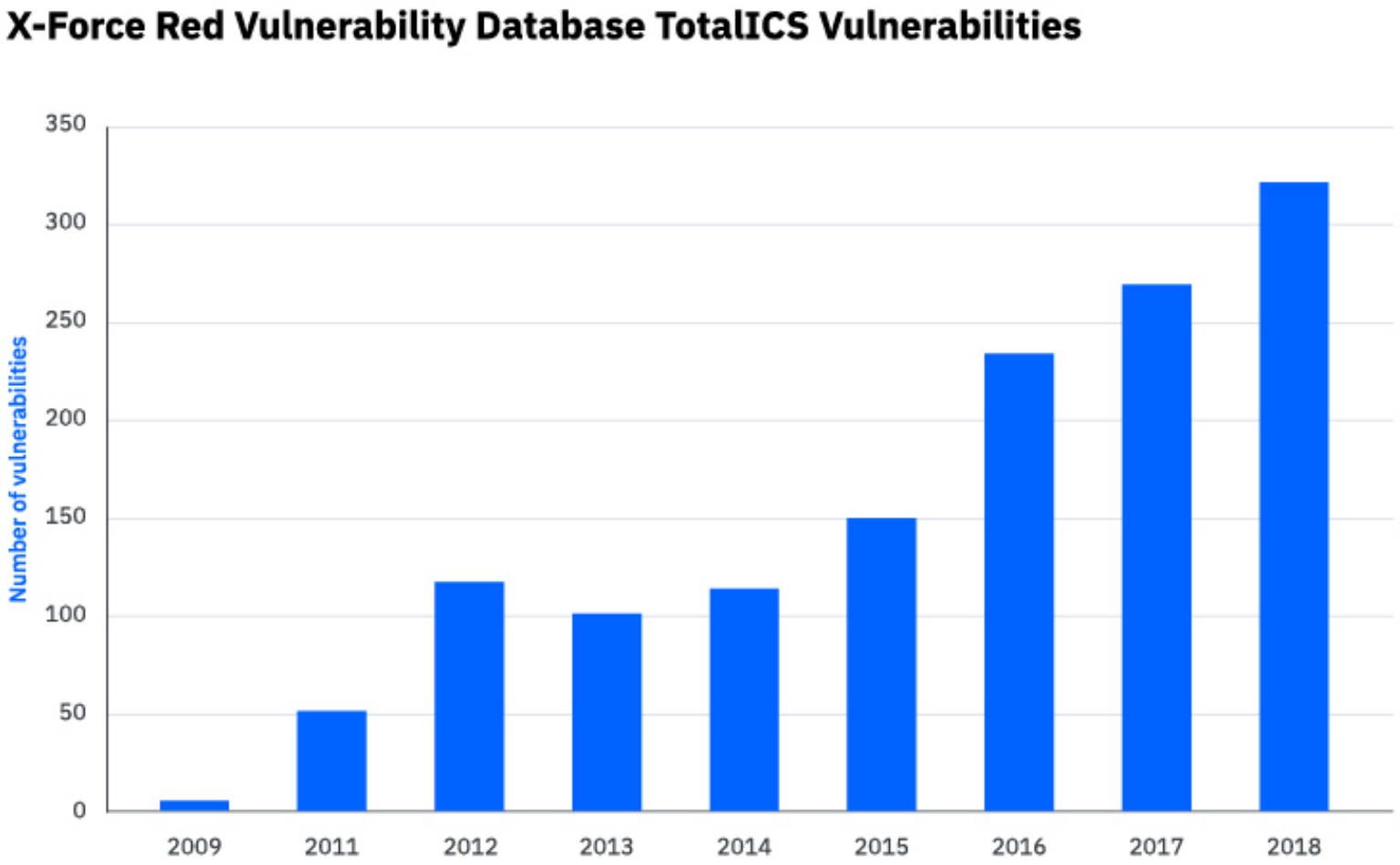
Analysis of and Mitigation Strategies for Real World ICS Security Incidents

Nico Fechtner

nico.fechtner@tum.de

July 9, 2020

Motivation: Growing ICS Threat Landscape



https://securityintelligence.com/posts/industrial-control-systems-security-to-test-or-not-to-test/

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

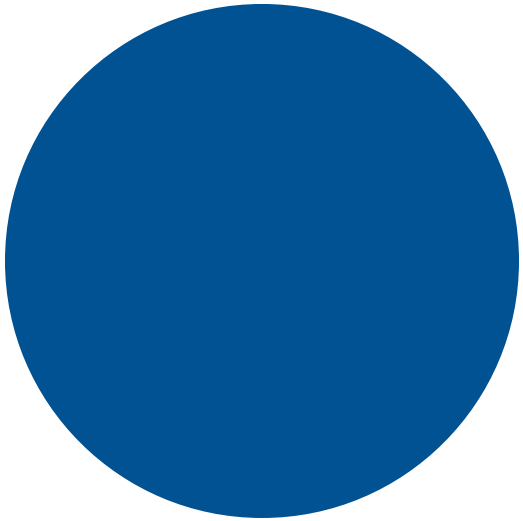
27 incidents analyzed (2000 - 2019)

Attack Type

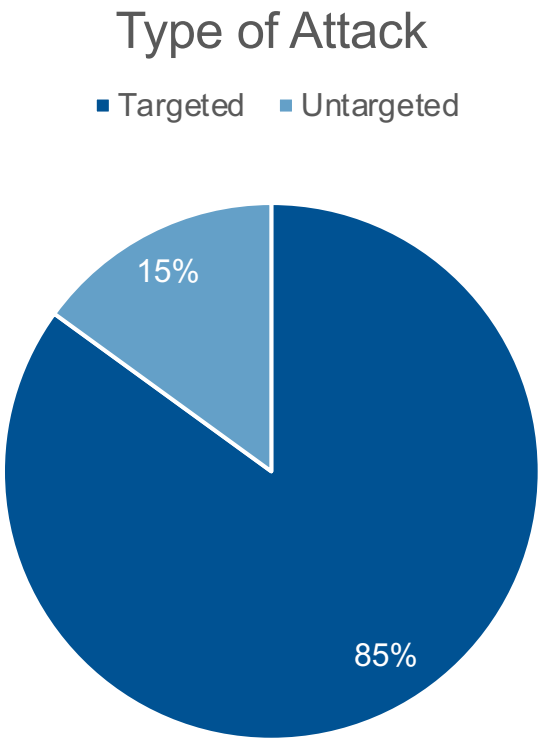
Targeted vs. untargeted

Attack Type

What percentage of attacks were targeted?

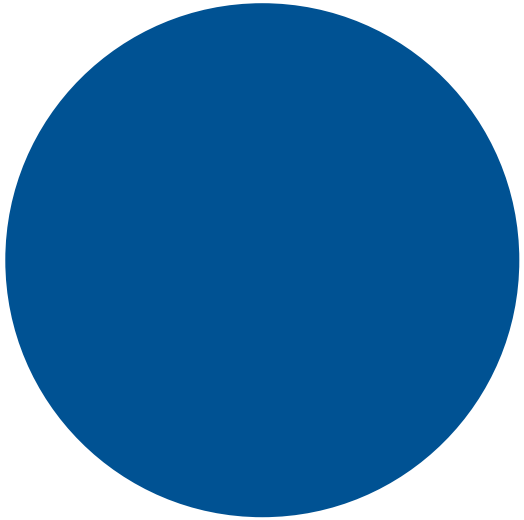


Attack Type

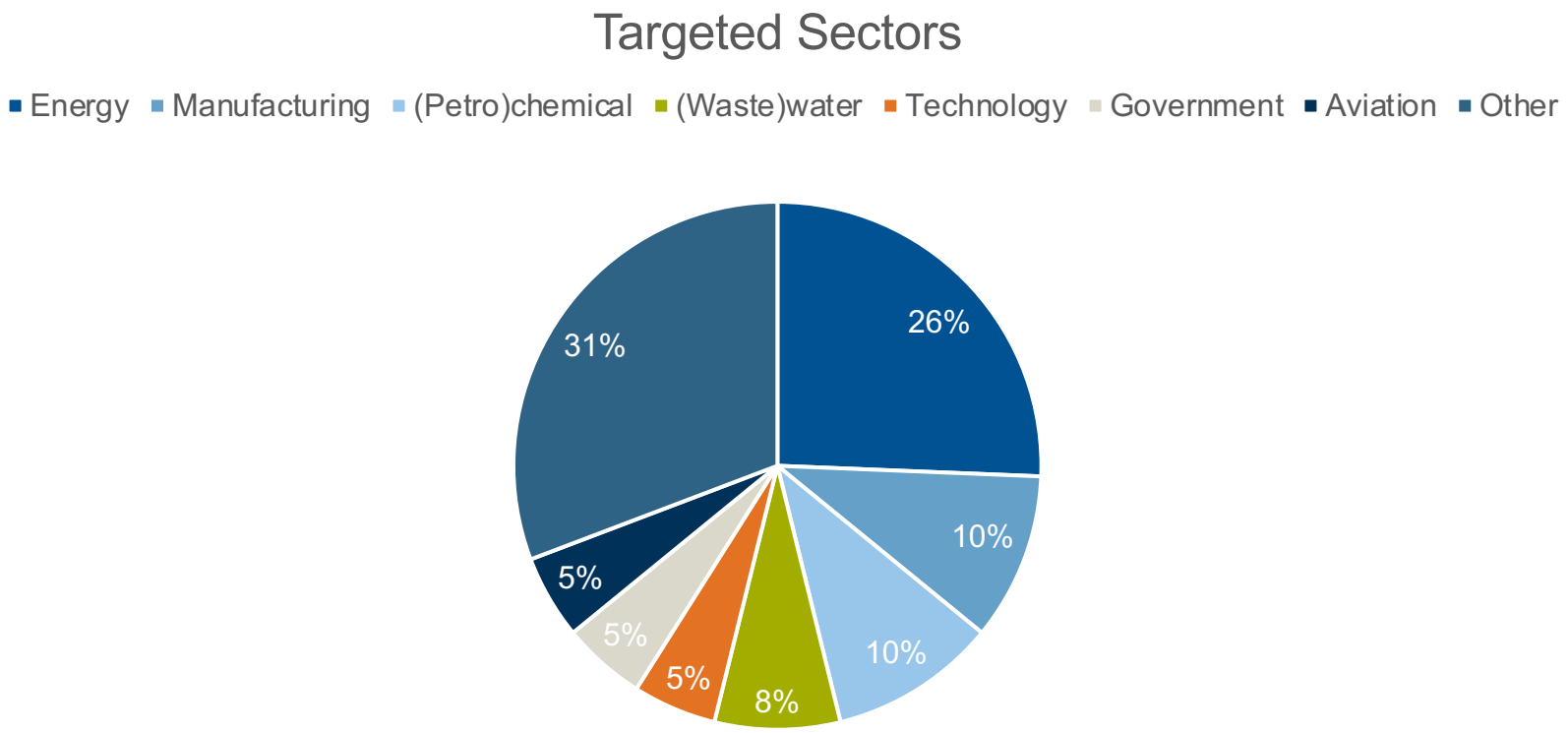


Targets: Economic Sector

Which economic sectors were affected most often (aviation, chemical, energy, water,…)?

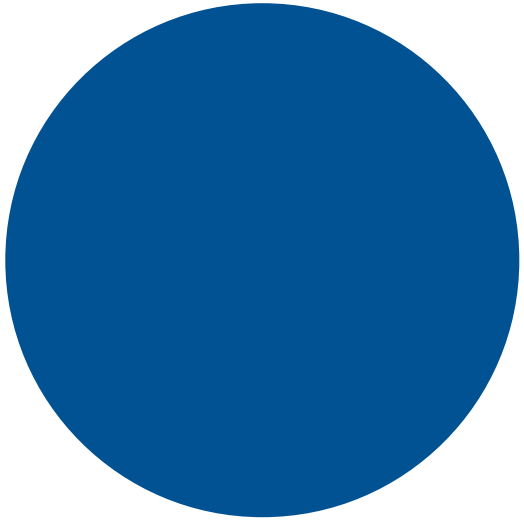


Targets: Economic Sector

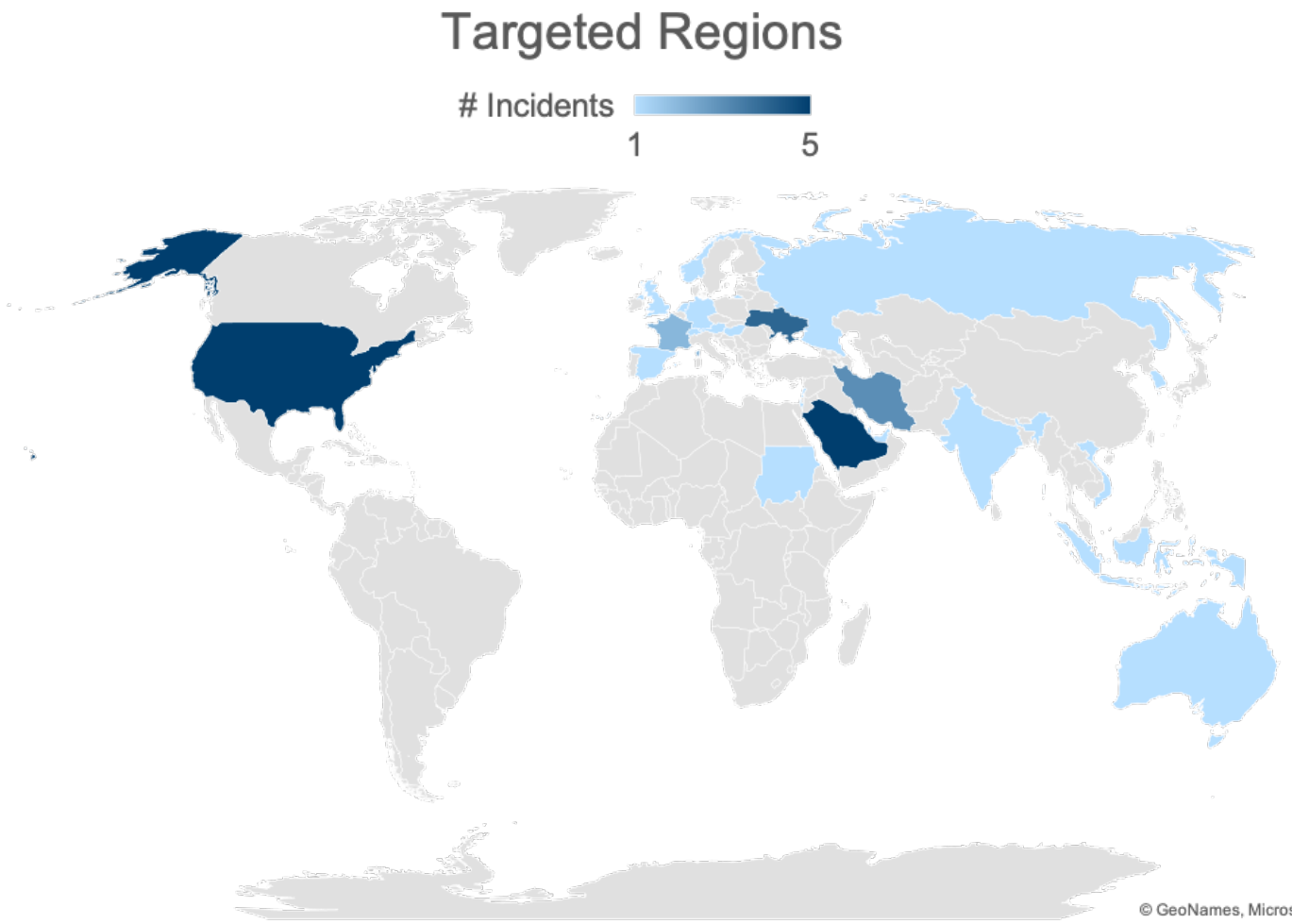


Targets: Geographic Location

Which countries/regions were affected most often?

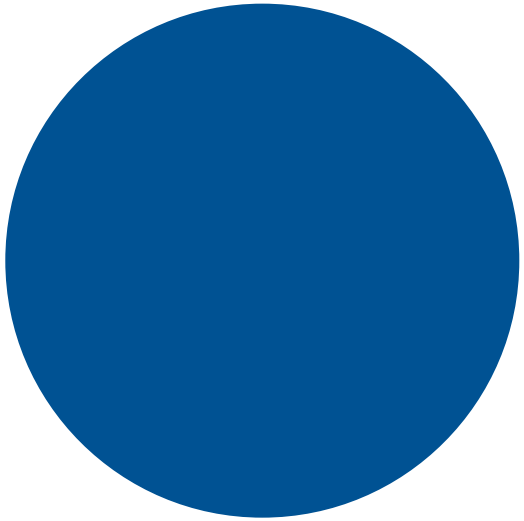


Targets: Geographic Location

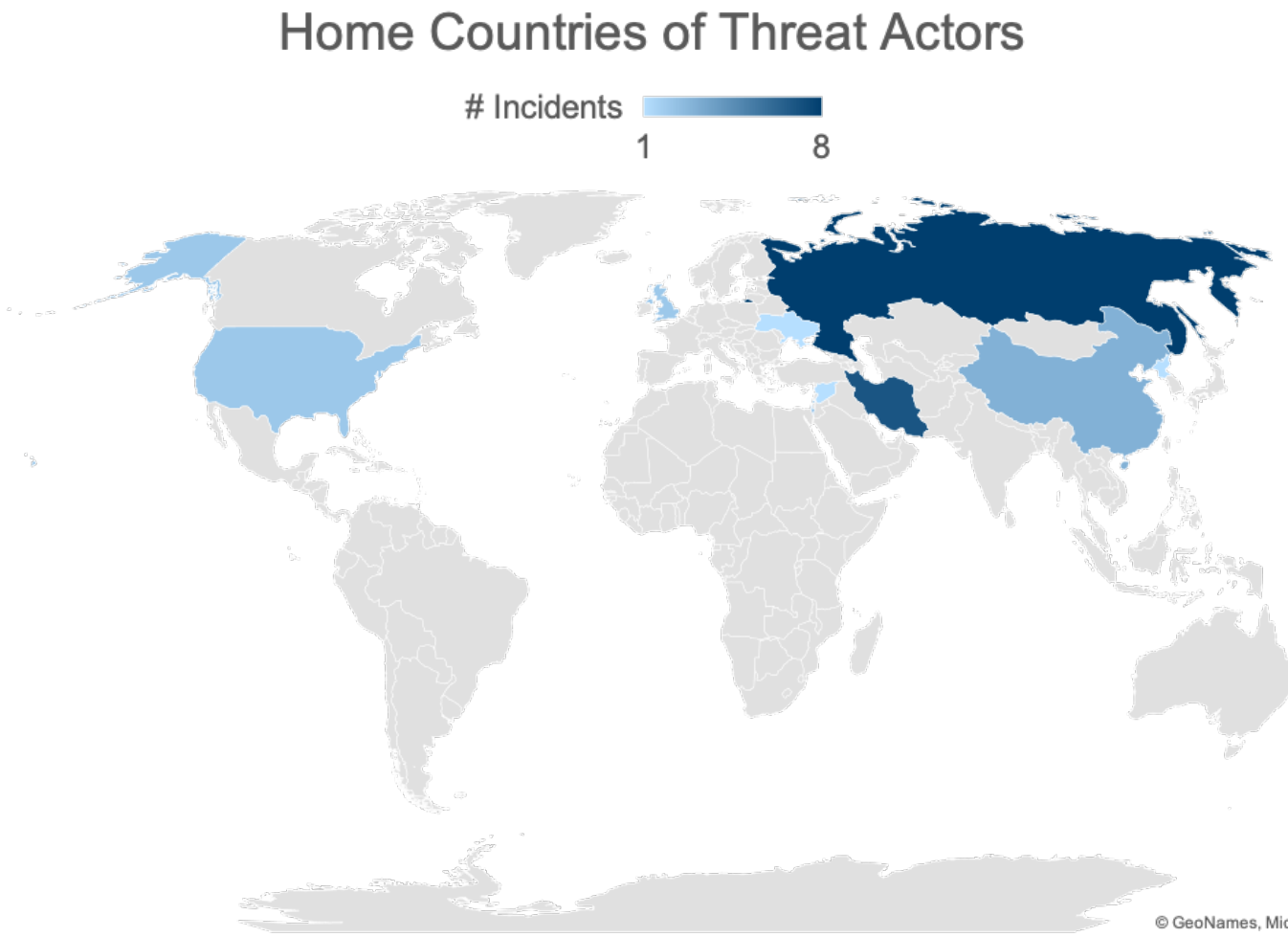


Threat Actors: Geographic Location

From which countries/regions do ICS attacks originate most often?

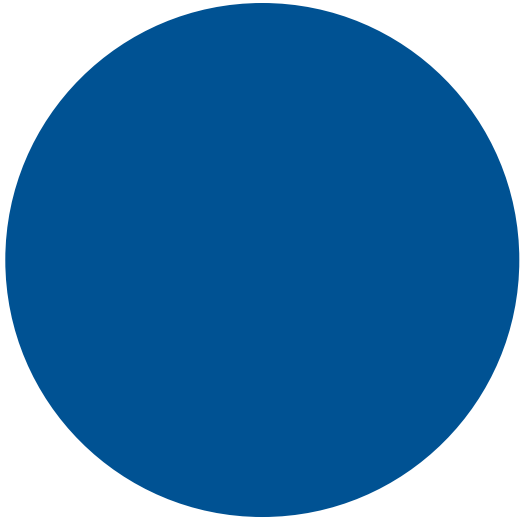


Threat Actors: Geographic Location

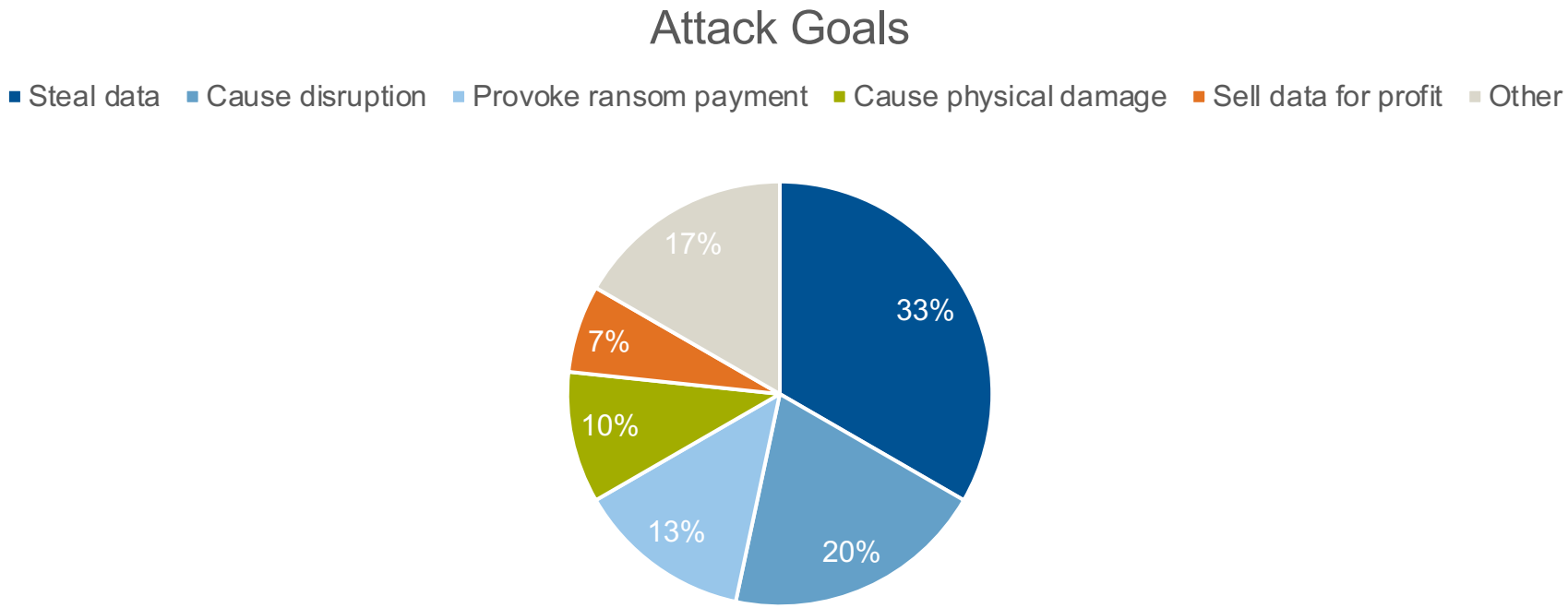


Attack Goals and Motivations

What are typical goals of ICS attacks?



Attack Goals and Motivations



Monetary Gain

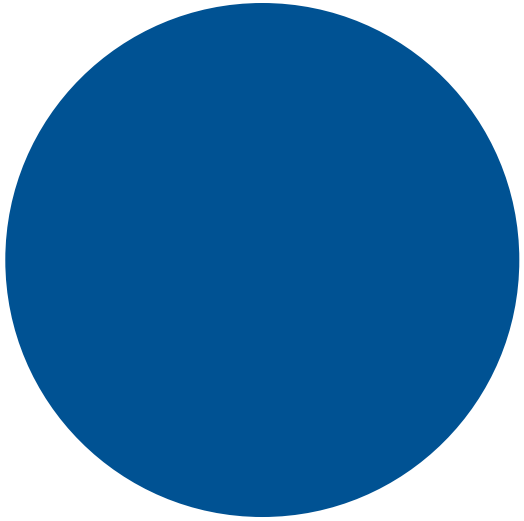
Information Gain

(Physical) Disruption

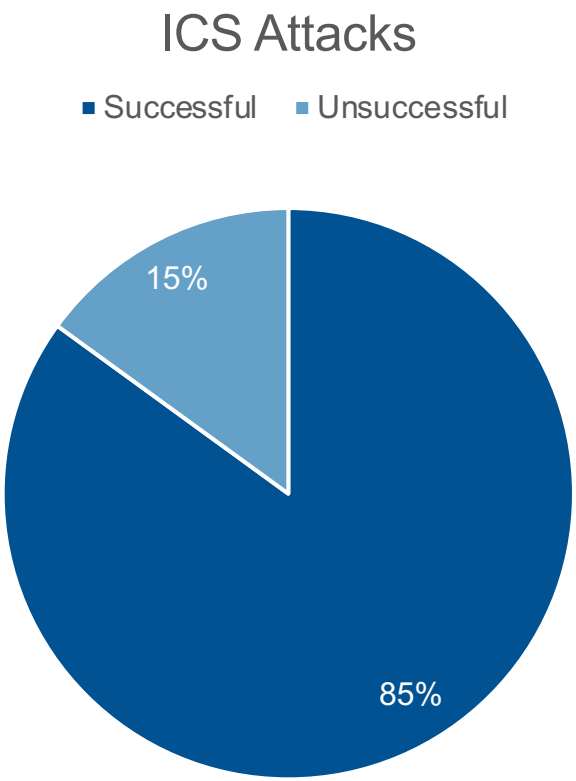
Attack Techniques

Success Rate

What is the success rate of ICS attacks?

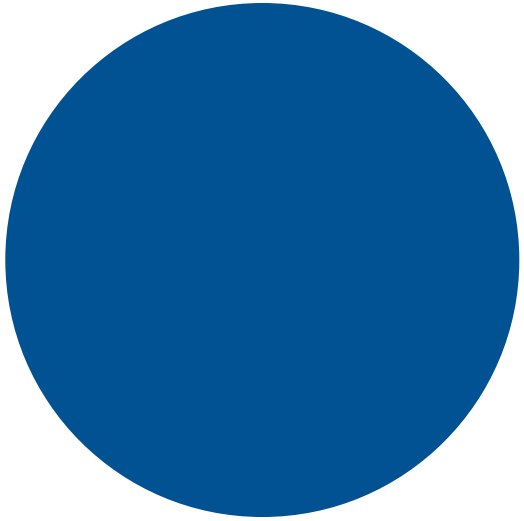


Success Rate



Dwell Times

How long does it take from the initial breach to the execution of the final ICS payload?



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

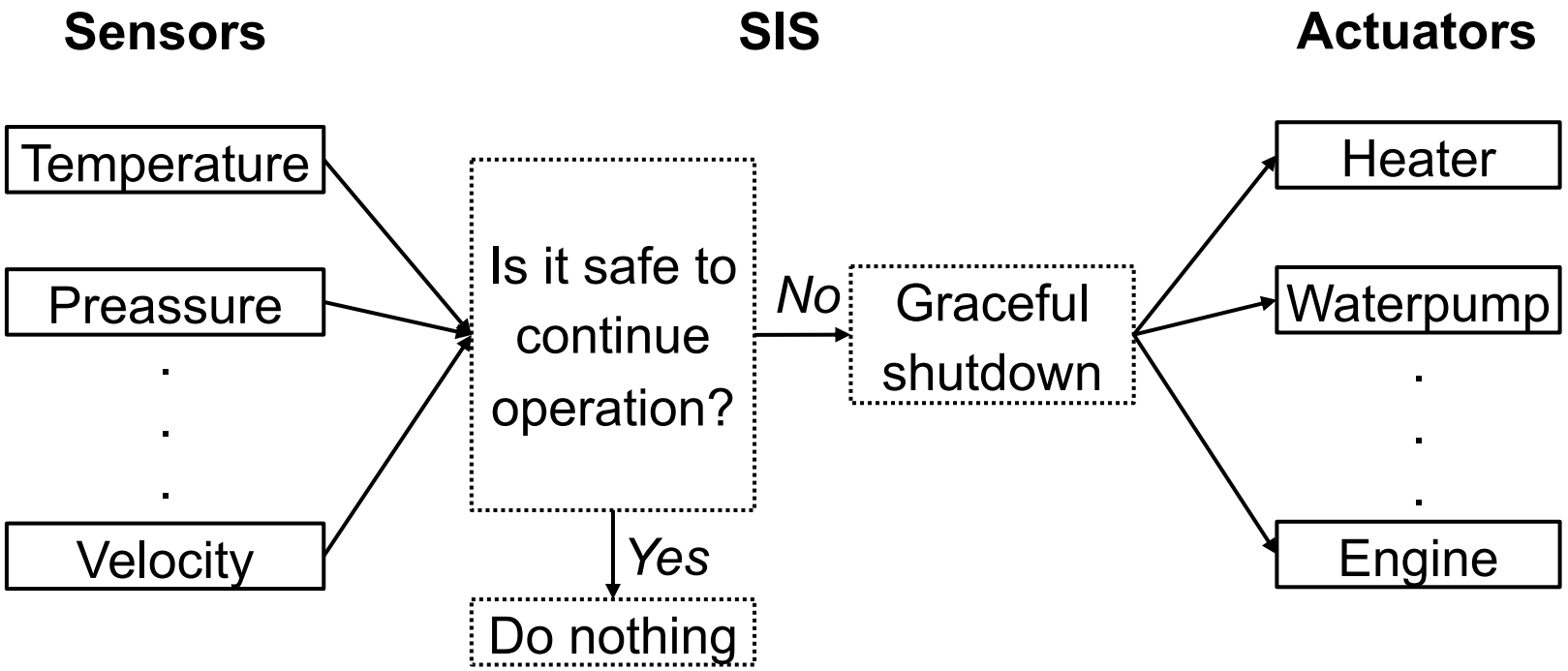
- Proper network segmentation
- Reliable backup strategy
- Up-to-date asset inventory
- Intrusion detection/prevention systems (IDS)
- Vulnerability management solutions

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.



The Triton Attack

- Target: Saudi Arabian oil refinery operated by Petro Rabigh
- Time of first impact: 2017

http://mcgtechtalk.com/wp-content/uploads/2017/03/spear-phishing.png

Attack and Response Strategies

- Still unclear how the ICS network got breached in 2014; possibly through spearphishing

http://mcgtechtalk.com/wp-content/uploads/2017/03/spear-phishing.png

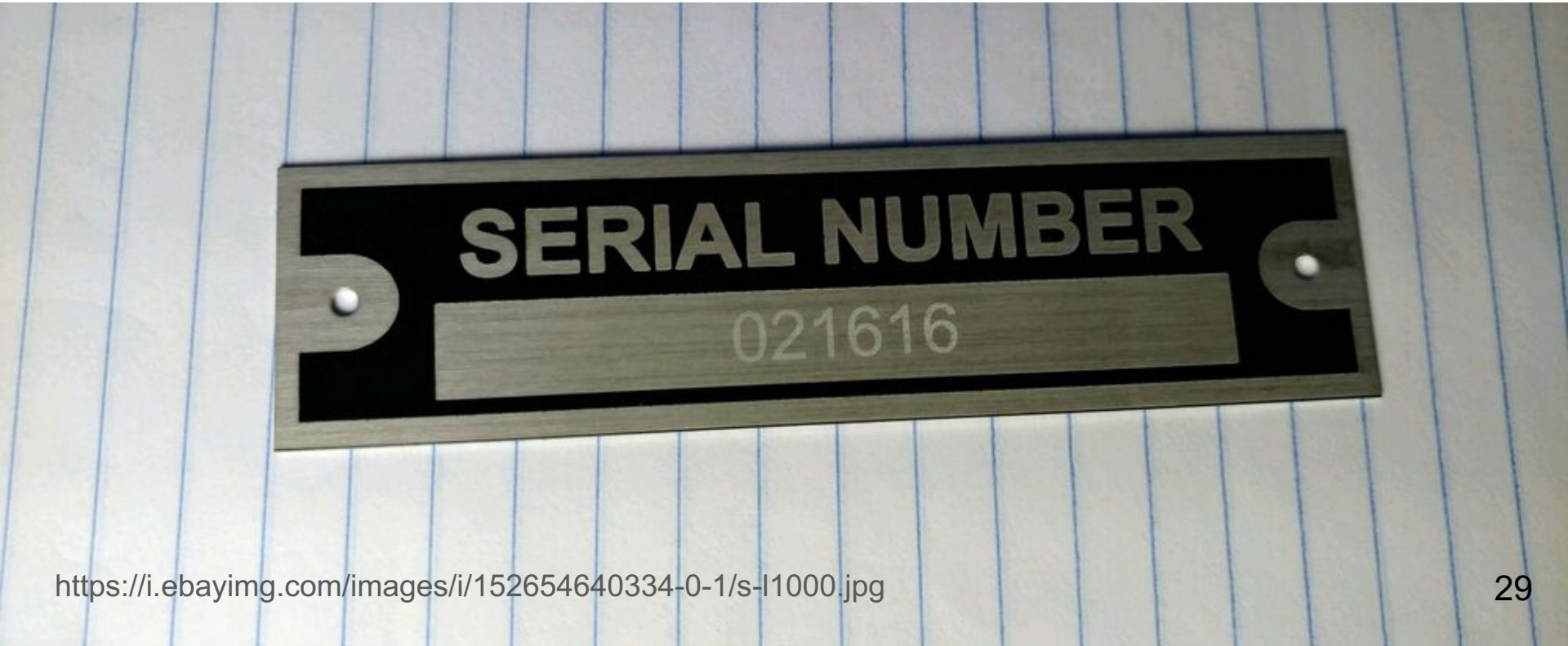
Attack and Response Strategies

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

https://manageditservicesminneapolis.com/importance-computer-network-maintenance-repair-info/

Attack and Response Strategies

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



https://i.ebayimg.com/images/i/152654640334-0-1/s-l1000.jpg

Attack and Response Strategies

- Since the SIS ran in *programming* instead of *run* mode, the Triton malware could be installed

http://hw-img.datpiff.com/m580a552/A-Mase_Two_Years_Later-front-large.jpg

Attack and Response Strategies

- After installation and execution, the plant tripped gracefully

https://unstrangemind.files.wordpress.com/2016/03/shutdown.jpg

Attack and Response Strategies

- Due to a human error, the malware contained a bug

https://www.beningo.com/wp-content/uploads/2016/03/AdobeStock_100096286.jpeg

Attack and Response Strategies

- After some investigations, the plant was brought up again

https://betanews.com/wp-content/uploads/2016/11/Restart-button-keyboard-key-e1479117780695.jpg

Attack and Response Strategies

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

https://betanews.com/wp-content/uploads/2016/08/install-software-laptop.jpg

Attack and Response Strategies

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

https://unstrangemind.files.wordpress.com/2015/03/shutdown.jpg

Attack and Response Strategies

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

https://www.cbronline.com/wp-content/uploads/2017/02/Investigation.jpg

Goals, Impacts, and Attribution

- Goal: remains unclear; probably causing disruption; potentionally threatening human lives
- 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

- Attacks are spread across multiple sectors and geographic regions
- Key threat actors reside in Russia and the Middle East
- The most common goals of ICS attacks are data extraction and causing disruption
- Important trends in terms of attack techniques are spearphishing, zero-day exploits, sophisticated obfuscation and evasion techniques, and exploiting Windows/AAD vulnerabilities
- Attackers usually reside in the victims' network for several weeks or months before executing the final payload

Conclusion

- Proper network segmentation
- Reliable backup strategy
- Up-to-date asset inventory
- Intrusion detection/prevention systems (IDS)
- Vulnerability management solutions

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

Fraunhofer AISEC

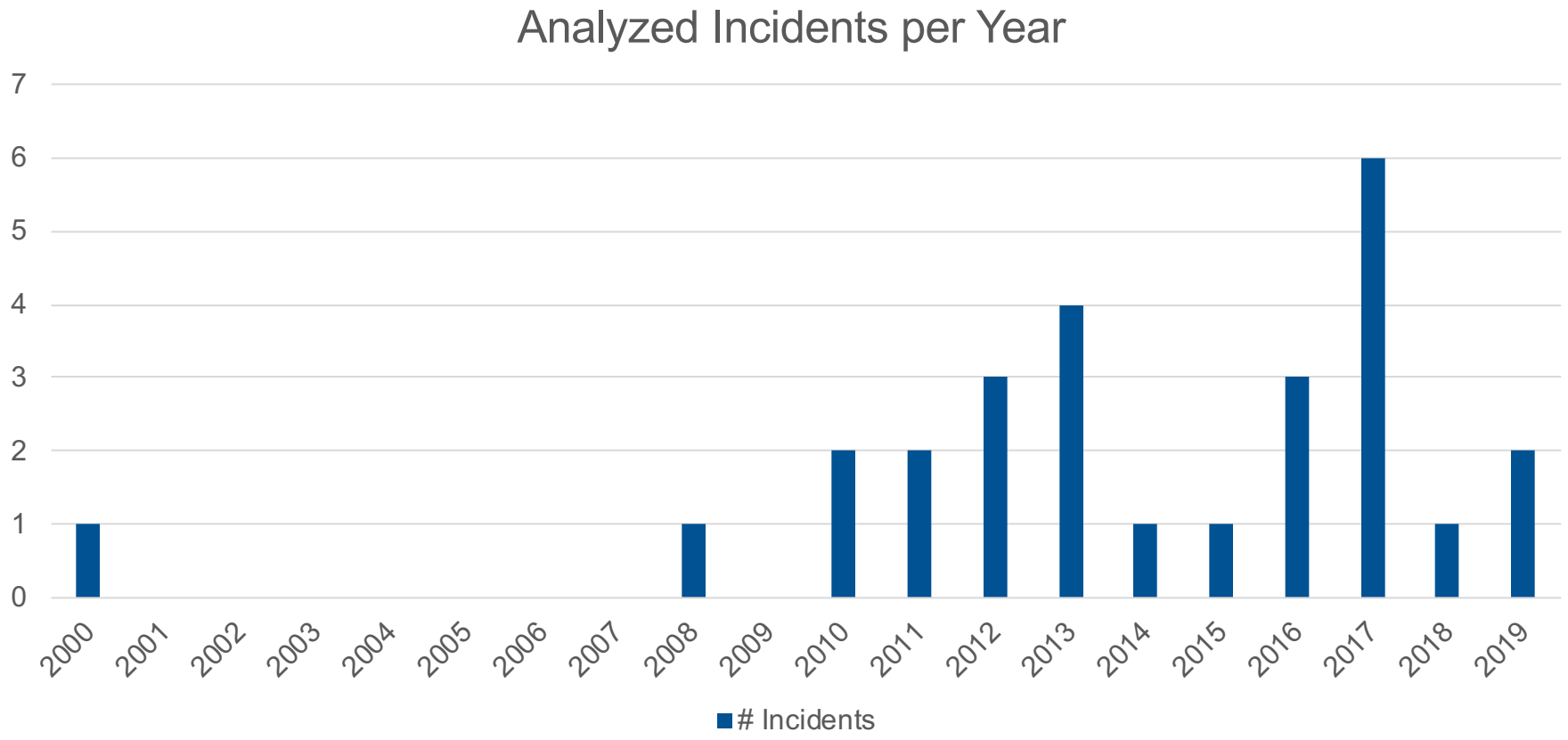
Q & A

Q & A

- In your research for this semniar, have you come across interesting ICS security incidents?
- Do you have further suggestions on how the Triton attack could have been prevented?

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

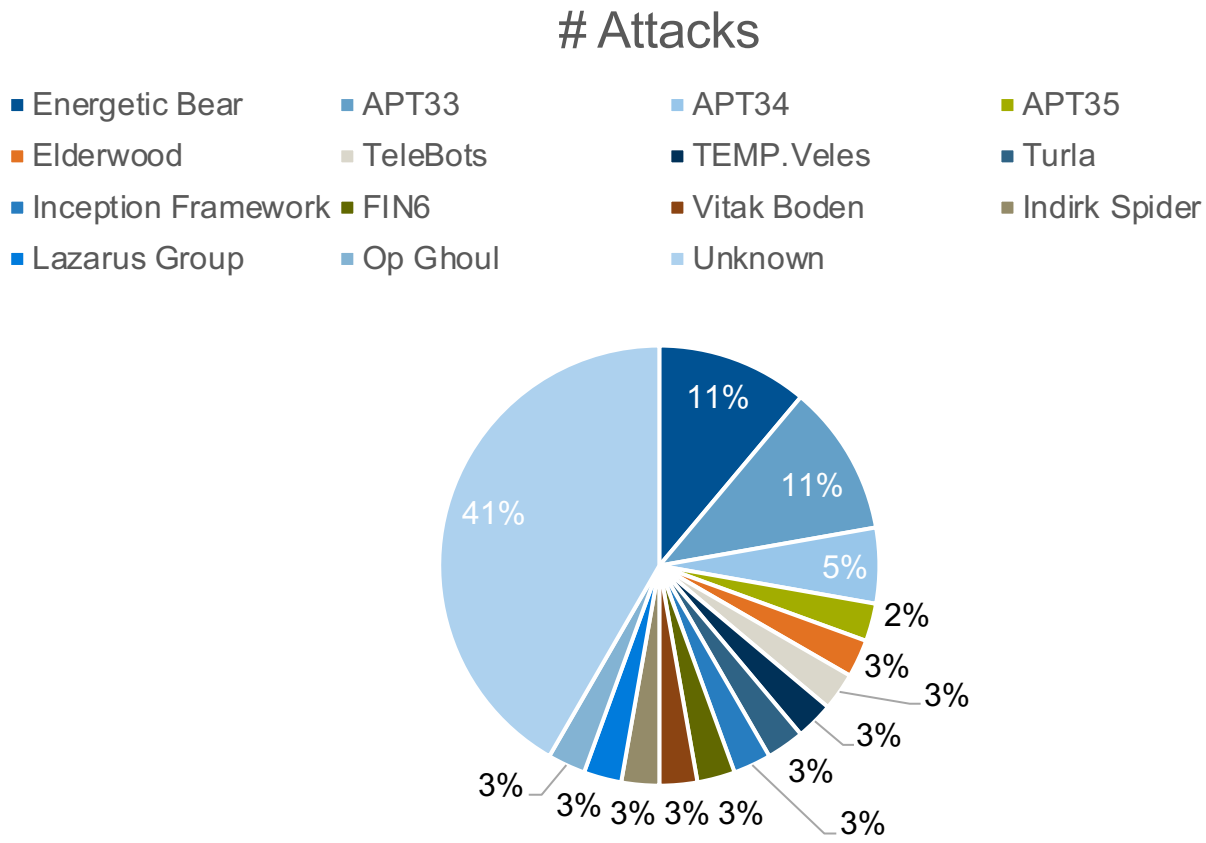
Analyzed Incidents

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

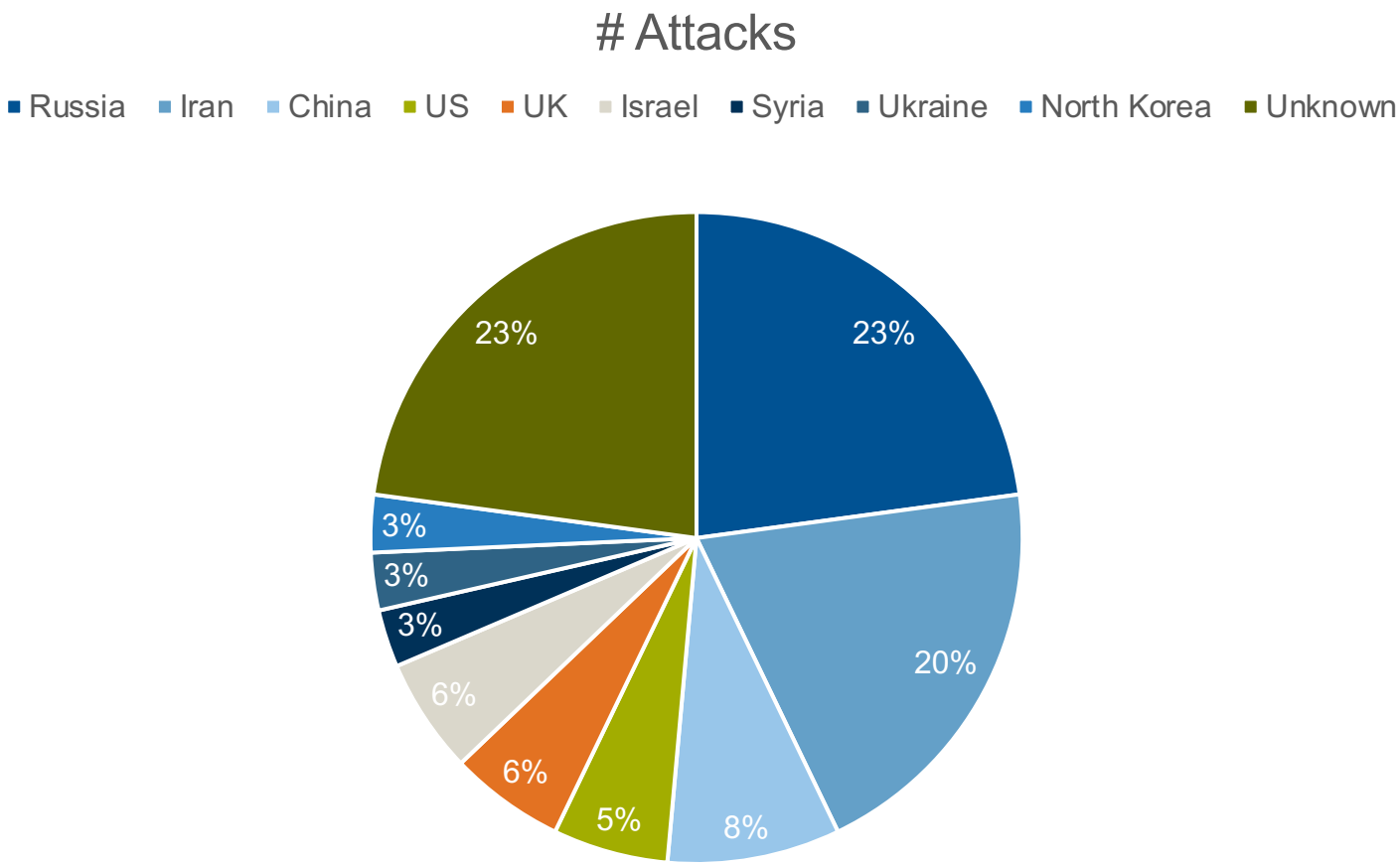
Targets: Economic Sector

- Aviation
- Energy
- Government
- Manufacturing
- (Petro)chemical
- (Waste)water
- ...

Threat Actors: Threat Groups



Threat Actors: Geographic Location



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
- Since the SIS ran in *programming* instead of *run* mode, the Triton malware could be installed

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 finally able to identify and remove the malware