Analysis of and Mitigation Strategies for Real World ICS Security Incidents

Nico Fechtner

Technical University of Munich &
Fraunhofer Institute for Applied and Integrated Security
nico.fechtner@tum.de

Abstract. More and more Industrial Control Systems (ICS) are getting connected to enterprise IT networks and the internet. Due to this, the attack surface of these systems increases, which led to a high number of real world ICS security incidents over the last years. It is therefore crucial to analyze and learn from past incidents to avoid common mistakes and to develop efficient detection and mitigation strategies that help to prevent future incidents. To support this process, this paper proposes a systematic comparative overview of historic ICS security incidents and an in-depth analysis of the Triton incident. Key findings include the following. Untargeted ransomware attacks as well as targeted state-sponsored operations both present prevalent threats to the ICS landscape. Adversaries often use techniques like spearphishing, zero-day exploits, sophisticated obfuscation and evasion techniques, and living off the land tools to extract data and cause disruption. Suitable defense strategies include increasing the security awareness of employees, strictly separating the ICS network from the enterprise IT network, and establishing a reliable backup strategy.

Keywords: ICS Security · ICS Attacks · Threat Actors · Triton.

1 Introduction

Industrial Control Systems (ICS) are used in a wide variety of industries such as food and agriculture, energy, water, transportation, chemical, nuclear power, pharmaceutical, and discrete manufacturing [18]. Initially, they were not connected to the internet and strictly separated from enterprise IT networks. Due to this isolation, it was hard, if not impossible, for adversaries to remotely attack ICS, which is why until recently security was not a big concern to companies running ICS. However, the attack surface of many ICS changed within the last two decades since they got connected to traditional IT networks and the internet—sometimes intentionally, sometimes by mistake. Inevitably, this led to an ongoing series of ICS security incidents.

While more and more of those incidents are reported, it is business-critical to develop suitable detection and mitigation strategies. An essential baseline in this process is analyzing and learning from past incidents. This is crucial to avoid

common mistakes and to effectively prevent future incidents. To support this process, this paper proposes a systematic comparative overview of historic ICS security incidents focusing on various parameters including targets, threat actors, attack techniques, goals and impacts, dwell times, operator reactions, and detection and mitigation strategies. The overview aims at identifying common attack patterns that could be used to prevent future attacks. To the best of the author's knowledge, such an overview has not yet been published.
Additionally, the Triton incident of 2017 is analyzed in detail to showcase how attackers perform sophisticated ICS attacks and which detection and mitigation strategies can be derived from their methodologies.

The remainder of the paper is structured as follows. Section 2 provides an overview of related work in the area of ICS incidents, which is used as the basis of the comparative overview that is provided in Section 3. Exemplary the Triton incident is analyzed in detail in Section 4. Section 5 concludes the paper by summarizing key findings and suggesting directions for future work.

2   Related Work

There are four main types of publicly available sources that provide information on ICS security incidents. First, there are incident enumerations like the Risi Database[1] and the ICS-CERT Alerts[2]. Second, ICS security companies like Dragos [7] and CyberX [3] publish yearly ICS threat reports discussing relevant incidents. Third, dedicated scientific papers are focusing on specific ICS incidents like the attacks targeting the Ukraine power grid [4] or the Triton malware [5]. Fourth, there are numerous blog posts, press releases, and conference talks covering ICS incidents. In addition, there is the MITRE ATT&CK ICS database[3] which includes information on tactics, techniques, and software used by threat groups to perform ICS attacks. Furthermore, there is a paper proposing an overview of historical ICS security incidents [10]. However, it is slightly dated and, more importantly, does not compare the different incidents systematically. All of the above-mentioned sources are taken into account to achieve exactly this in the upcoming section.

3   Comparative Overview of ICS Security Incidents

From the literature and resources stated in Section 2, a total of 27 ICS security incidents were extracted. Those are the basis of the following analysis and can be found in Table 1. Note that due to incidents not being reported, the high number of incidents that are reported and new incidents occurring steadily, this table is inherently incomplete, but rather tries to focus on the most prevalent attacks

---

[1] https://www.risidata.com/Database

[2] https://www.us-cert.gov/ics/alerts

[3] https://collaborate.mitre.org/attackics/index.php

launched until February 2020. The following subsections provide a comparative overview of these incidents. Each subsection aims to compare the incidents with regards to specific attributes, e.g. the involved threat actors or the utilized attack techniques.

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

Table 1. ICS incidents considered in the comparative analysis ordered by the time of their first impact.

3.1   Targets

When analyzing the entities affected by ICS security incidents there are two fundamentally different kinds of attacks that have to be considered separately. On the one hand, there are targeted attacks against unique entities. Making up roughly 85% of the analyzed incidents, targeted attacks seem to present a diverse threat landscape to ICS and are therefore analyzed in detail below. On the other hand, there are untargeted attacks. Here, the threat actors are not

interested in the specific entities that will be affected by the attack, but rather aim for as many incidents as possible. Often this is achieved by a self-replicating component within the malware used for the attacks. While only four of the analyzed incidents fall into this category, they still pose a significant threat to ICS. Interesting to see is that the malware used for untargeted attacks usually is not tailored specifically for ICS environments, but rather targets common operating systems like Microsoft Windows and enterprise networks in general. Many instances of untargeted attacks fall in the category of ransomware. For example, the popular WannaCry ransomware spread not only to desktop computers around the world but also infected a series of ICS workstations e.g. at a Taiwanese manufacturing plant leading to outages due to encrypted hard drives [16]. This kind of incidental infections of ICS systems with malware originally intended for enterprise networks are becoming more and more of a threat in recent years [7], [3], [19].

Since untargeted attacks are not aimed at specific entities but often solely intend to infect as many systems as possible, e.g. with self-replicating components, there is in general no pattern observable in terms of the geographical location or the economic sector of the affected parties. Targeted attacks, however, can be analyzed for such patterns.

When it comes to the geographical location of ICS attack victims, the most affected regions seem to be Europe and the Middle East. Companies located in Europe are targeted by about 37% of the analyzed attacks. The country affected the most until now is Ukraine falling victim to multiple attacks targeting its power grid. The Middle East is being targeted by about 33% of the analyzed attacks. In about 19% of the analyzed incidents, the US were amongst the victims. Note that while being home to important global threat actors as discussed in Subsection 3.2, neither Russia nor China nor North Korea report a lot of ICS incidents against entities located in their countries.

When it comes to the economic sectors falling victim to targeted ICS attacks, the most affected one is the energy sector being targeted in at least 37% of the analyzed targeted attacks. Often, those operations include attacks against power grids like the attacks taking place in 2014 and 2015 in Ukraine. Other examples of targeted entities within the energy sector include oil and gas pipelines as well as refineries. The remaining victims of ICS attacks are spread across a wide variety of other economic sectors including manufacturing, water, petrochemical, governmental organizations, and transportation.

3.2   Threat Actors

In total, at least 16 specific threat actors were involved in the analyzed ICS incidents according to the current state of research. When it comes to the threat actors responsible for ICS attacks there is the fundamental issue of attribution. Usually, threat actors want to stay anonymous and do not confess performed attacks. Therefore, there are often only conjectures about the threat actors involved in certain attacks. In line with that, 37% of the analyzed attacks cannot be associated with a specific threat actor. Furthermore, it is often difficult to

locate threat actors geographically, since they usually apply various techniques to hide their physical location [11]. With regards to the analyzed incidents, 33% of the threat groups cannot be associated with a specific country. It can be said, however, that 30% of all analyzed attacks are assumed to originate from Russia and 22% from the Middle East, thereof 67% from Iran. Other countries being home to important threat groups are China, the US, and North Korea. The most active threat actors according to the sample of incidents taken into account here are Energetic Bear from Russia, being involved in at least 15% of all attacks, and APT33 from Iran, being involved in at least 11% of all attacks. Interesting to note is that some threat groups primarily act on their own while others tend to collaborate with others. For example, APT33 often collaborates with other Iranian threat groups, whereas Energetic Bear mostly acts on its own. When it comes to the team size, only one threat actor corresponds to a single person—Vitak Boden in the Maroochy Water incident. Since this incident in the year 2000, ICS attacks got a lot more sophisticated which is why the team size of threat groups continues to grow.

At least 59% of the analyzed attacks are considered to be performed by government-funded threat actors. On the one hand, targeted ICS attacks require a large amount of knowledge and resources to which often only state-sponsored groups have access to. On the other hand, governments can profit in various ways from ICS attacks against foreign countries, be it through industrial espionage, by making critical facilities and infrastructures unavailable or even by targeting human lives. ICS attacks are therefore sometimes even considered an act of war [14].

3.3   Attack Techniques

An established model to characterize ICS attacks is the ICS Cyber Kill Chain depicted in Figure 1. It is comprised of two stages. In stage one, IT intrusion preparation and execution happens, i.e. the attacker compromises the IT network and positions herself in the ICS network. This stage can be completed without specific knowledge about ICS technologies or protocols. In stage two, ICS attack development and execution are performed, e.g. an attack targeting certain actuators—for example, water pumps—is developed, tested, and executed.

When it comes to the initial access in stage one of the ICS Cyber Kill Chain, two attack techniques seem to be most popular among the analyzed incidents. The first one is spearphishing, which was reportedly performed in at least 26% of the attacks. The second one is the utilization of zero-day exploits, which was observed in at least 11% of the attacks. When inside the victims' IT network, attackers often use common software. For example, in at least 11% of the cases, Mimikatz was used for credential capturing. Popular exploitation frameworks like Metasploit and Cobalt Strike are frequently used, too. More recent trends are the use of sophisticated obfuscation and evasion techniques and *living off the land* tools—like PowerShell or PsExec—to avoid being detected by Intrusion Detection Systems (IDS).
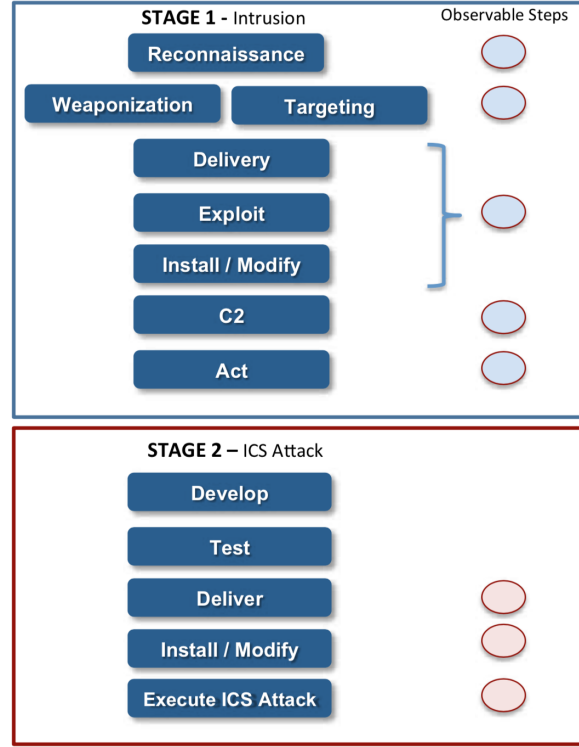
Fig. 1. ICS Cyber Kill Chain as introduced by the SANS institute, from [2].

Since untargeted attacks usually rely on ransom- or wiperware, they do not go beyond stage one of the ICS Cyber Kill Chain. Targeted attacks, however, aim more and more often to exploit specific ICS environments, which requires the attackers to first gain access to the ICS network. One possible way to pivot is lateral movement via Windows authentication services. Once in the ICS network, a multitude of different exploit strategies has been reported. Most adversaries attack ICS components like Programmable Logic Controllers (PLCs) or Safety Instrumented Systems (SIS) to modify their behavior or to make them fail altogether. Doing so, they are often able to control actuators like water pumps, fake the values of sensors, or turn off the power supply. To make disaster recovery harder, attackers often wipe Human-Machine Interfaces (HMIs), too. While according to the ICS Cyber Kill Chain stage one typically has to take place before stage two, there is an example where the attack was performed the other way around. In 2013, an unknown attacker stole login credentials of a third-party heating, ventilation, and air conditioning (HVAC) contractor of US Target Stores. From the ICS network, the adversary then pivoted into the IT network to install credit card stealing software. [10]
One important trend in addition to the techniques described above is the trend

away from manual attacks specifically tailored for a single victim towards more victim-agnostic ICS attack frameworks enabling scalable attacks. A case in point are the attacks on the Ukraine power grid. The first attack in 2015 was exclusively manual and the effort put into it could not be directly utilized for attacks against other energy infrastructures. One year later, however, there was a second attack targeting the power grid, but this time the adversaries had developed a framework, which in theory allows them to scale their attack to a multitude of different victims with a relatively small effort. [9]

3.4 Attack Goals and Realized Impacts

The most common goal of adversaries is to extract data from the victim's systems. 37% of all analyzed attacks were designed to achieve exactly this. Other goals often pursued by attackers are to cause disruption (22%), to provoke a ransom payment (15%), and to cause physical damage (11%).
When it comes to the underlying motivations of attackers, three distinct ones seem to dominate. First, attackers often strive for monetary gain. This motivates ransomware attacks like WannaCry or LockerGoga as well as information stealing with the goal of selling the data to the highest bidder. Second, some adversaries are interested in the data they steal themself and do not intend to sell them. This motivates ICS espionage operations like StoneDrill were Iranian threat groups gathered intelligence about Saudi Arabian ICS environments. Third, there are threat actors that intend to disrupt the regular operation of ICS by causing outages or even physical damage. The latter was e.g. the case in the famous Stuxnet incident in 2010 where the US and Israelian government attacked nuclear enrichment facilities of Iran to sabotage the possible development of nuclear weapons. Untargeted attacks falling into this category are typically related to wiperware which erases or encrypts hard drives without a subsequent ransom demand.
In total, a minimum of 85% of the attacks are considered to be at least partly successful in achieving their goals with regards to some of their victims. Typical impacts include information loss, financial loss—via physical damage, ransom payment or costly recovery processes—and environmental damages. Fortunately, until to date, there are no ICS incidents known that killed humans.
One incident considered to be unsuccessful is the well-known Triton attack, which failed for reasons not fully understood up until today. Section 4 provides a detailed analysis of the incident and its impacts. Furthermore, untargeted attacks often partly fail to achieve their goal since a lot of companies can restore operations without a long outage or paying a ransom thanks to sufficient backup strategies.

3.5 Dwell Times and Reactions

Dwell time describes how long an adversary is in a system before the actual attack payload is executed. In the context of untargeted attacks, the dwell time usually is a matter of days, while when speaking about targeted attacks, it typically ranges from multiple months, e.g. in the attacks targeting the Ukraine

power grid and the Triton incident, to multiple years. The latter is considered to be the case, for example, when considering the Red October espionage campaign against multiple countries initiated by a Russian threat actor. It seems that with dwell times this long it should be possible for the ICS network operators to detect that something is wrong within their systems before the adversaries deliver the final payload. Unfortunately, while this holds in theory, attacks are usually not detected in their early stages in practice. There are some cases—BlackEnergy and Triton—where the administrators were able to detect that something is wrong before the actual attack payload was executed, but in most cases, the attack is only detected after the final exploit was already delivered.

When it comes to reacting to an untargeted attack, there is sometimes the option to pay a ransom to get the hard drives decrypted again by the adversary. While this should be avoided, since there is no certainty that the attackers will indeed decrypt the hard drives as promised, there are still cases known were the ransom was paid. The typical response to a destructive untargeted attack, however, is to restore operations from backups. In the case of targeted attacks, when operators suspect that an intrusion has happened, they often shut down the ICS to prevent further breaches, physical damage, and threats to human lives. This happened, e.g. in the Triton incident. When the final payload was already delivered by the adversaries, however, often the only thing left to do is to start recovery processes that aim to restore operations and typically also include digital forensics to analyze how the incident could have happened, e.g. how the ICS network could be breached, in the first place.

3.6   Detection and Mitigation Strategies

To be able to detect ongoing ICS attacks, the first fundamental resource is an up-to-date asset inventory. Only with that, possibly dangerous activities can be detected. Such detection is usually offered by IDS that lookout, e.g. on network tabs or SPAN ports, for anomalies in the network traffic. Compared to traditional IT networks, this is a quite promising approach, since—in contrast to IT networks—the expected network traffic does not vary much such that false positives can be relatively easy tuned to a minimum. A more active approach to IDS is threat hunting where security specialists try to identify adversaries that already reside inside the victims' network.

When it comes to suitable mitigation strategies, the first line of defense to strengthen are the humans operating ICS. As stated in Subsection 3.3, many adversaries use social engineering for gaining an initial foothold in the victim's network. The risk of successful phishing compromises can e.g. be reduced by security awareness workshops. More on the technical side of things are vulnerability management solutions. In ICS environments, it is often not that easy to patch hosts, since this could mean downtime and therefore revenue loss. However, it is crucial to at least know which hosts have known vulnerabilities. Even if a patch might not be possible, one could e.g. at least harden the network segmentation around the vulnerable hosts to make a compromise less likely. Inspired by traditional IT networks, firewalls are becoming more and more popular

in ICS environments, too. They are especially critical in overlapping parts of the IT and ICS networks. Last but not least, it is essential to have a solid backup strategy that allows for restoring operations fast and reliable, e.g. in the case of a ransom- or wiperware attack.

4   Detailed Analysis of the Triton Attack

While the previous section conducted a comparative overview of the most prevalent ICS security incidents to highlight general trends, this section focusses on a specific attack to detail how insight gained from such an analysis can be used to prepare for future attacks. Exemplary, the Triton attack targeting a Saudi Arabian petrochemical plant in 2017 is analyzed. The incident—also known as Trisis [6] and HatMan[4]—is chosen as an example since it is considered to be of significant importance to the ICS community [6]. Most importantly, it was the first attack targeting SIS and therefore potentially threatening human lives. In addition, the attack was highly sophisticated, and even when it was eventually detected by the plant operators, they were not able to stop it immediately.

4.1   Attack and Response Strategies

When it comes to Triton, the details of stage one of the ICS Cyber Kill Chain are still unclear. It seems that the IT network of the Petro Rabigh oil refinery got breached already in 2014, however, the exact techniques used for the initial access and the movement into the ICS network are not unambiguously known. It is suspected, however, that the initial access happened via a spearphishing attack [15].
Stage two of the ICS Cyber Kill Chain began shortly after the initial breach of the IT network when the attackers managed to access the Triconex SIS from Schneider Electric—therefore the name Triton or Trisis. SIS are an integral part of ICS in that their sole purpose is to maintain safe operations should failures of other hard- or software occur. They should prevent catastrophic incidents like explosions or fire and protect human lives [5]. It is therefore crucial that this last line of automated safety defense operates correctly. The inputs for an SIS are sensors measuring physical values e.g. temperature, pressure, or rotation speed. In real-time, the SIS analyzes these values and outputs a single decision: if it is safe to continue operation. Should the SIS decide that there is an unsafe physical condition, suitable commands are sent to according actuators like water pumps, machine engines, or valves. [6]
To protect an SIS from unintended modification, there is a physical keyswitch controlling the mode of operation. Under normal circumstances, this switch should be set to *run*, which disables arbitrary changes to the logic of the SIS. In the case of Petro Rabigh, however, the switch was set to *program mode*, which allows for logic changes. Why this was the case is unknown, but it might have

---

[4] https://www.us-cert.gov/ics/MAR-17-352-01-HatManSafety-System-Targeted-Malware

been the case that an engineer programming the SIS simply forgot to switch it back to *run* mode. In addition to these modes of operation, network connectivity to an SIS should, in theory, be extremely limited if existent at all. In practice, for example, plant operators sometimes want to retrieve data from SIS to analyze them, which is why they allow for more network connectivity than needed for reasons of convenience. This might have been the case at Petro Rabigh, too. [6] After the adversaries had found out the exact type of SIS the plant was using, they left for about two years and developed the targeted malware that came to be known as Triton. Thereafter, they returned and installed the malware on the SIS. The goal of Triton was to change the internal logic of the SIS, which could lead to severe consequences. It could, for example, reprogram the SIS in a way such that it would not shut down the plant in the case of an emergency. [13] Indeed, shortly after the malware was installed, the SIS tripped and shut down the oil refinery. However, this shutdown was not intended by the attackers. It turned out that it was rather the consequence of a programming error on their side, which instead of rewriting the logic of the SIS brought it down entirely, which led to a shutdown of the whole plant. The plant operators in charge at this point did not consider the SIS failure as being the result of a targeted ICS attack. Instead, they thought it must be some error of the SIS itself. So they contacted the SIS vendor and hired some investigators, however, none of them was an ICS security specialist. In the end, they were not able to identify the root cause of the shutdown and considered it to be a one time error. Eventually, they brought up the refinery again. [13] This meant that the adversaries got a second chance to attack. Indeed, they were able to identify the bug, which made the Triton malware fail in the first attempt. They tried to fix this bug and attacked the SIS again. Just like a few weeks before, the SIS tripped and the refinery was shut down again. In hindsight, it turned out that the attackers did not correctly fix the bug. So essentially, the attack finally failed due to human error. After the SIS tripped a second time, the plant operators brought in ICS security specialists which were able to identify that the SIS was infected with malware.

4.2   Goals, Impacts, and Attribution

As of today, the motivations behind the Triton attack remain unclear. However, since the adversaries specifically targeted the SIS, it is likely that the goal was to cause disruption. One way to achieve this is to provoke a shutdown of the plant, which also happens to be the actual impact of the attack. In total, the oil refinery was out of operation for multiple weeks. While this also implied monetary losses for the companies running the petrochemical plant, financial gain or harm does not seem to be the driving force behind the attack [12]. Another way of creating disruption is to cause an unsafe physical state leading to physical damage [6]. Potentially this could also lead to threats against human lives. Whether or not the latter was indeed part of the adversaries' goals is still unknown. The reasoning about the underlying motivations together with the fact that the attack required a lot of resources suggests the threat actor behind the attack to

be state-sponsored [12]. Indeed, the attackers behind the Triton operation seem to be a Russian threat group, given the name *TEMP.Veles*, which is probably backed by a Russian research institute based in Moscow [8], [17].

4.3   Detection and Mitigation Opportunities

If it should indeed be the case that the initial access happened via spearphishing, this would be a very common scenario that likely can never be remediated completely. An effective countermeasure, however, are continuous security awareness trainings to help employees identify phishing attacks [1].

When it comes to ICS security countermeasures, those focusing on SIS are especially promising. Two key strategies would potentially have stopped the Triton attack early on. First, an SIS should reside in a very restricted network segment allowing no unnecessary communication to workstations residing possibly even in the IT network. Second, SIS should–if not currently programmed by an operator—always be set to *run* mode and never to *program* mode. If the according keyswitch is set to *program*, operators should receive an alert. Additionally, SIS should be protected by physical access controls and devices to be directly connected to an SIS or the according network segment should be scanned for known malware beforehand. [6]

5   Conclusion

The comparative overview given in Section 3 and the detailed analysis of the Triton incident performed in Section 4 lead to the following key findings. First, not only operations targeting specific ICS environments but also untargeted attacks—e.g. in the form of ransomware—are becoming more and more a threat to industrial environments. Second, most of the ICS incidents are considered to be state-sponsored. Third, important trends in terms of attack techniques are spearphishing, zero-day exploits, sophisticated obfuscation and evasion techniques, and living off the land tools. Fourth, the most common goals of ICS attacks are data extraction and causing disruption. Fifth, attackers usually reside in the victims' network for several weeks or months before executing the final payload. Keeping these trends in mind, possible defense strategies include increasing the security awareness of employees, strictly separating the ICS network from the enterprise IT network, and establishing a reliable backup strategy. To build upon these results and to make them more precise it would be useful to include additional ICS incidents to the 27 that are already considered in the proposed overview. Additionally, it could be interesting to study how ICS companies manage to defend against known threats over the course of time. Core hypotheses to test would be if companies are more likely to defend their infrastructure successfully against a certain threat the longer it is publicly known and if so, how fast this adaptation of defense strategies happens. Furthermore, a comparison of detection and mitigation products from different vendors with an according evaluation—possibly utilizing ICS honeypots—could be considered.

References

1. Arachchilage, N.A.G., Love, S.: Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior **38**, 304–312 (2014)
2. Assante, M.J., Lee, R.M.: The industrial control system cyber kill chain. SANS Institute InfoSec Reading Room **1** (2015)
3. CyberX: 2020 global iot/ics risk report (2020)
4. Defense Use Case: Analysis of the cyber attack on the ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC) **388** (2016)
5. Di Pinto, A.A., Dragoni, Y., Carcano, A.: Triton: The first ics cyber attack on safety instrument systems. In: Proc. Black Hat USA. pp. 1–26 (2018)
6. Dragos: Trisis malware: Analysis of safety system targeted malware. Tech. rep. (2017)
7. Dragos: 2019 - year in review: The ics landcape and threat activity groups (2020)
8. FireEye Intelligence: Triton attribution: Russian government-owned lab most likely built custom intrusion tools for triton attackers (2018), https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html, [Online; accessed 09-May-2020]
9. Greenberg, A.: Crash override: The malware that took down a power grid (2017), https://www.wired.com/story/crash-override-malware/, [Online; accessed 03-May-2020]
10. Hemsley, K.E., Fisher, E., et al.: History of industrial control system cyber incidents. Tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States) (2018)
11. Huang, K., Siegel, M., Madnick, S.: Systematically understanding the cyber attack business: A survey. ACM Computing Surveys (CSUR) **51**(4), 1–36 (2018)
12. Kovacs, E.: New 'triton' ics malware used in critical infrastructure attack (2017), https://www.securityweek.com/new-ics-malware-triton-used-critical-infrastructure-attack, [Online; accessed 09-May-2020]
13. Lee, R.: The industrial cyberthreat landscape: 2019 year in review (2020), https://youtu.be/yIFf27yL-p4, RSA Conference
14. Lindsey, N.: Iranian hackers apt33 now threatening ics security (2019), https://www.cpomagazine.com/cyber-security/iranian-hackers-apt33-now-threatening-ics-security/, [Online; accessed 11-May-2020]
15. Nohe, P.: What if getting phished could kill you? (2019), https://www.thesslstore.com/blog/what-if-getting-phished-could-kill-you/, [Online; accessed 09-May-2020]
16. Skybox Security Inc.: Tsmc wannacry hits ot plants with a hefty price tag (2018), https://blog.skyboxsecurity.com/tsmc-wannacry/, [Online; accessed 27-April-2020]
17. Sobczak, B.: The inside story of the world's most dangerous malware (2019), https://www.eenews.net/stories/1060123327, [Online; accessed 09-May-2020]
18. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ics) security. NIST special publication **800**(82), 16–16 (2011)
19. Zimba, A., Wang, Z., Chen, H.: Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. Ict Express **4**(1), 14–18 (2018)