



VB2020
localhost

30 September - 2 October, 2020 / vblocalhost.com

HELLO FROM THE OT SIDE!

Daniel Kapellmann Zafra

FireEye Mandiant, USA

danielkapellmann.z@fireeye.com

ABSTRACT

Throughout the last 10 years, those working in the nascent operational technology (OT) security community have consistently strived to highlight the unique characteristics that differentiate them from information technology (IT) security professionals. Stressing the differences between the two communities has increased awareness about the various challenges we face to protect industrial control systems (ICS) and critical infrastructure. However, recent analysis of major OT security incidents and attacker techniques, tactics and procedures (TTPs) sheds light on the need to re-evaluate this posture.

Most sophisticated attacks on OT systems leverage computers, servers, standard operating systems and IT protocols as conduits – or what *Mandiant Intelligence* calls ‘intermediary systems’ – to their ultimate targets. This infrastructure is often used as an avenue to impact physical assets and processes. As a result, defenders’ advanced IT security skills represent a unique opportunity to explore and understand the intrusion methods, or TTPs, that take place across the OT attack lifecycle.

In this paper, I discuss a series of cases observed by the *Mandiant* Cyber Physical Threat Intelligence team that showcase the impact of IT threats on OT security and highlight challenges that can only be solved by understanding both computing equipment and process automation. This paper encourages security professionals to embrace a new perspective and bring their skills to task on some of the most compelling challenges in cyber physical security.

HELLO FROM THE OT SIDE!

It has been ten long years since the Stuxnet worm was first uncovered and operational technology (OT) security was recognized as a discipline. During this decade, we have not only seen the first incidents designed to cause a physical impact, but also the evolution of public and private organizations protecting critical infrastructure and industrial production. We have observed advances in vulnerability reporting, information sharing, the study of tactics, techniques, and procedures (TTPs), and the consolidation of a high-skilled research community.

While there are multiple reasons to feel positive about the future of OT security, we continue to face significant challenges. The most significant of these are the lack of expertise and solutions to protect physical processes in the midst of an increasing integration of IT and OT systems. For ten years, we heard many reasons why IT and OT systems are not the same, requiring different security measures [1]. While this narrative raised awareness about the uniqueness of OT security, little has been discussed about the intersection of the two disciplines. By highlighting the importance of this point, we invite security professionals to find solutions for some of the most compelling challenges in OT security.

THEY SAY THAT IT/OT INTEGRATION SUPPOSED TO HEAL YA

The main purpose of OT is to monitor and control physical processes [2]. While this task used to rely solely on analog engineering equipment and human labour, it now depends on much more than sensors, actuators and controllers. IT and OT systems are increasingly converging, partly mobilized by market demand calling for greater production efficiency. Most communication across devices that are critical to production currently travels through common networking and computing equipment. Furthermore, continuous production in highly scalable industries, such as manufacturing, requires uninterrupted streams of data exchanged between assets such as data historians, manufacturing execution systems (MES), and other business process management systems (BPMS) [3]. Losing access to this data can result in loss of process visibility, delaying or stopping production.

Seen from a security perspective, the integration of IT systems along physical production processes results in a significant increase in the attack surface. It makes it feasible for threat actors to interact remotely with processes using the same tools they would use for other types of data compromises. Ideally, one could avoid this by not adopting data-driven IT solutions in industrial environments. However, this is not a feasible solution for users because IT systems are perceived to enable significant business efficiencies for scaling production and distributing services. Said differently, current market practices privilege usability and scalability over safety and security.

While IT/OT convergence generates benefits, it also poses threats that did not used to be of concern for industrial producers, such as ransomware or cryptomining, which have impacted OT organizations across different verticals. More importantly, in most highly sophisticated attacks reaching the core of OT networks, the actors leverage computers and servers, using the same or similar operating systems and protocols as used in IT as a conduit – what *Mandiant* calls ‘intermediary systems’ – to their ultimate targets. Truly understanding and preventing these incidents requires a unique combination of both IT and OT security expertise.

WE’RE CALLING TO TELL YOU OT STORIES THAT KEEP US AWAKE AT NIGHT

As previously explained, the convergence of IT-based solutions with OT processes results in a large attack surface that we currently struggle to defend. Perhaps the best way to illustrate this challenge is by sharing some of the cases we commonly observe in the OT security intelligence community. In September 2019, *Mandiant* released the Operational Technology

Cyber Security Incident Ontology (OT-CSIO) in an attempt to categorize the different types of threats we have observed impacting OT systems [4]. From the cases incorporated in this assessment, which represent the most well-known OT incidents and some generic examples, only a couple impacted specialized industrial equipment on levels 0 and 1 of the Purdue Model of Reference Architecture (PERA) [5]. The rest of the cases categorized by this model represent common IT threats that do not require any understanding of the underlying physical processes, but may still result in undesirable outcomes.

OT CYBER SECURITY INCIDENTS MATRIX

ATTACK	SOPHISTICATION	IMPACT				
		Compromise	Data Theft	Degradation	Disruption	Destruction
Targeted	Low	Logging into internet-connected devices (e.g. using Shodan)	Threat actors selling VNC access to SCADA systems	Russian scientists arrested for mining cryptocurrencies at Federal Nuclear Center in Sarov		Shamoon
	Medium	TEMPIsotope Reconnaissance Campaign			Maroochy Shire Sewage Spill and Ukraine 2015 Post-compromise ransomware campaigns (e.g. Megacortex, LockerGoga, or Ryuk)	Ukraine 2015
	High				Ukraine 2016 TRITON Attack	Stuxnet
Non-Targeted	Low	Financially-motivated actor inadvertently accesses internet-connected HMI while conducting mass scanning / brute forcing of RDP/VNC servers		Cryptomining Malware on European Water Utility Portable Executable File Infector Malware Impacting Windows-based OT assets	WannaCry Infection on HMIs	
	Medium					
	High					



Figure 1: OT Cyber Security Incidents Matrix [4].

The following sample of cases selected from OT-CSIO illustrates some of the main areas of opportunity for collaboration between IT and OT security. Some of the challenges described below may appear simple from the perspective of securing data. However, by analysing the implications of these cases in terms of their impact on critical physical processes, we are faced with an entirely different narrative.

Post compromise ransomware deployment

The analysis of incidents where ransomware deployment resulted in disrupted physical production is one of the best examples where we could benefit from joint IT and OT expertise. Since at least 2017, we have seen a significant increase in ransomware incidents where industrial or critical infrastructure organizations were forced to delay or stop the supply of end products and services. In the beginning, we observed widespread infections such as WannaCry and NotPetya, where Windows-based human-machine interfaces (HMIs) and engineering workstations were infected. Although in most cases the impact was minor, some organizations, such as *Maersk*, suffered severe consequences, resulting in financial loss and production delays [6].

From 2018 to 2020, we observed an evolving threat landscape where actors shifted from opportunistic to post-compromise ransomware deployment. Following this strategy, an actor relies on the same tactics for broad distribution of malware to obtain initial access to a variety of victim environments. Once in a network, they focus on privilege escalation to explore the best paths forward to deploy ransomware [7]. In cases where the actor cannot monetize financial or customer data, the disruption of production processes offers an alternative path to generate profits.

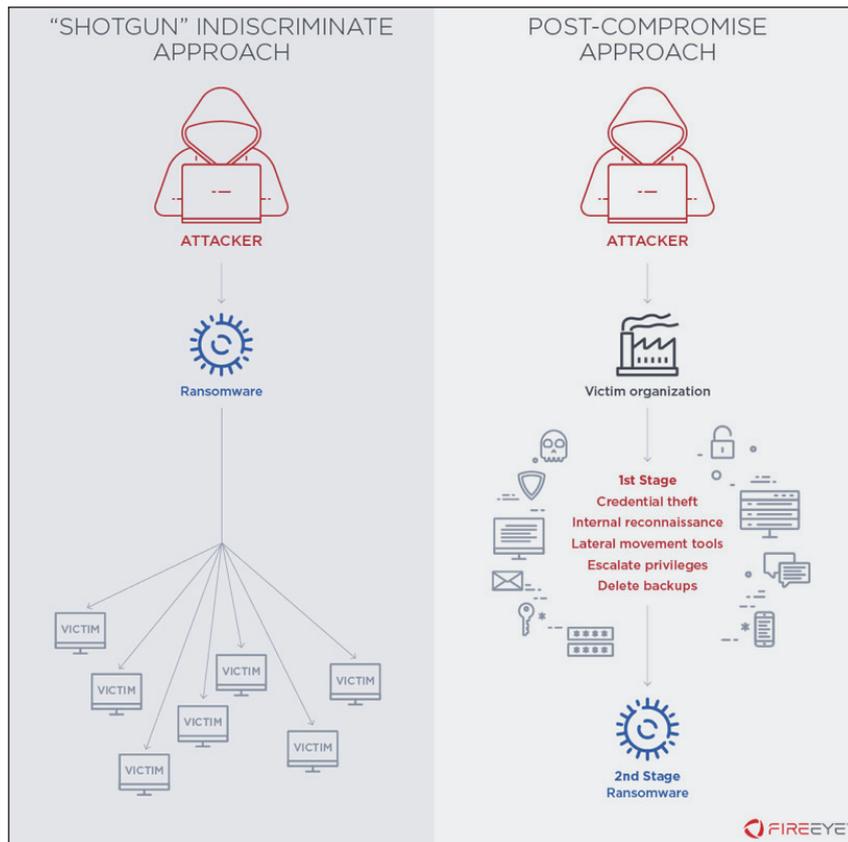


Figure 2: Comparison of indiscriminate vs. post-compromise ransomware approaches [7].

The phenomenon of ransomware impacting physical production can best be explained when analysed from a combined IT and OT perspective. This is best illustrated by the sequence of events that led different security research groups to analyse and eventually understand the SNAKEHOSE (aka SNAKE or EKANS) ransomware.

An IT security team first uncovered a SNAKEHOSE ransomware sample likely in a malware analysis platform [8]. Thankfully, the security team identified and publicly disclosed that the malware deployed a process kill list, which included some processes related to OT.

In response, OT security teams moved quickly to analyse the list of ~60 industrial processes included in the kill list. Analysis only from the OT perspective determined that the SNAKEHOSE ransomware was designed to target industrial processes and described the relevance of those specific assets [9].

Joint analysis from our IT and OT security teams helped us realize that the truth was located somewhere between the two versions. The process kill list was much longer than reported, including over 900 IT processes. It had also been deployed alongside at least three additional ransomware families in previous incidents impacting industrial organizations [7]. Based on this information, we determined that the OT processes identified in these lists were likely coincidental output of automated process collection from target environments and not a targeted effort to impact OT. However, we cannot rule out that the actors may have at least some level of understanding of what these processes were used for.

At the time, the process kill list had likely joined the lines of commodity malware and had been deployed with minor modifications next to samples of at least six ransomware families. The analysis was possible thanks to the support of Mandiant's reverse engineering team, who manually extracted the list from the function that was terminating the processes. We then developed further detections to identify similar abnormal behaviours.

By the time this paper is released in October 2020, the previously described list will likely be distributed in even more cases of post-compromise ransomware deployment impacting industrial organizations. Names such as LockerGoga, DoppelPaymer, Megacortex, Ryuk, Maze and Nefilim will continue to be heard regularly while we find solutions to address this challenge.

TRITON custom and commodity intrusion tools

As a second example, we selected TRITON, which is probably the most sophisticated OT incident observed in the wild [10]. Although the TRITON attack framework has mainly been recognized for its components developed to target *Triconex Safety Instrumented Systems (SIS)* controllers, most of the attack lifecycle relied on IT. Following the broad footprint left by

the attacker in IT systems across most, if not all, of the attack lifecycle, we developed an actor's TTP profile and provide context to the incident. We identified the group behind the intrusion [11], an estimated initial date of operation, and the set of custom and commodity tools that they used in at least a couple environments [12]. We also developed detections to hunt for similar activity, hopefully before the actor reaches other safety controllers.

TOOL	COMPONENTS	PURPOSE	ATTACK LIFECYCLE STAGE						
			Initial Compromise	Establish Foothold	Escalate Privileges	Internal Reconnaissance	Move Laterally	Maintain Presence	Complete Mission
SecHack	KB77846376.exe	Credential harvesting			X	X			
	KB77846376.exe.x64								
NetExec	NetExec.exe	Remote command execution							
	runsvc.exe	NetExec runner					X		
Cryptcat-based backdoor	cryptcat.exe cryptsvc.exe svchostpla.exe	Backdoor							
	compattelprerunner.exe	C&C domain name generator		X					
	ProgramDataUpdater.xml	Scheduled task file (persistence mechanism)							
PLINK-based backdoor	napupdatedb.exe	Backdoor		X					X
Bitvise-based backdoor	alg.exe userinit.exe csrss.exe	Backdoor							
	tquery.dll txflog.dll cryptopp.dll DEFAULT DEFAULT.BAK	Backdoor components					X	X	
OpenSSH-based backdoor	spl32.exe WinSAT.exe csrss.exe	Backdoor							
	clusapi.dll PolicMan.dll verifier2.dll misc.mof setup.ini	Backdoor components					X	X	
WebShell	logoff.aspx	Modified legitimate Outlook Web Access Component							
	flogon.js	Modified legitimate Outlook Web Access Component				X			X
	ftpexts.tlb	Output file containing credentials harvested by logoff.aspx							

Figure 3: Selection of custom tools used by the group behind the TRITON incident [12].

Although the TRITON incident would be much less concerning without its OT components, most of the tools utilized by the actor before reaching the final target were based on common *Windows* or *Linux*-based assets present in most OT and IT networks. This pattern has been seen across other major OT incidents, including leveraging computers to gain access to targeted programmable logic controllers (PLCs) (e.g. Stuxnet), interacting directly with Internet-connected human machine interfaces (HMIs) (e.g. BlackEnergy), and gaining remote access to an engineering station to manipulate a remote terminal unit (RTU) (e.g. INDUSTROYER).

Espionage and reconnaissance campaigns

Another opportunity for collaboration between IT and OT security teams is uncovering espionage and reconnaissance campaigns. Given the abundance of this type of activity across a variety of regions and industries, determining the scope of an espionage campaign is not always an easy task. The following three cases illustrate this challenge:

CASE	DESCRIPTION	DETERMINATION OF OT SCOPE
TEMP.Isotope 2017 [13]	Cluster of threat activity targeting energy and other critical infrastructure sectors leveraging spear-phishing and strategic watering holes.	<ul style="list-style-type: none"> • Spear phishing directed at engineers • Watering holes on strategic industry sites • Uncovered activity accessing HMIs and other process-related information
APT33 2019 [14]	Password-spraying attacks across thousands of organizations.	<ul style="list-style-type: none"> • Dozens of industrial equipment and software firms targeted (among other victims)
WildPressure 2020 [15]	Malicious campaign distributing Milum trojan across victims in the Middle East.	<ul style="list-style-type: none"> • At least some targets were related to the industrial sector



Table 1: Sample of publicly disclosed espionage and reconnaissance campaigns.

As observed in Table 1, obtaining evidence to determine the ultimate goals of espionage and reconnaissance campaigns is a difficult task and is often limited to the analysis of victimology. While in the first case intentionality is noticeable when grouping the TTPs with observed snippets of accessed information, in the second and third cases further details are needed to confirm explicit targeting focused on retrieving information about OT environments.

Regardless of these challenges, we highlight that all of the objects uncovered as evidence in this section were retrieved from sources such as emails, websites, network traffic, and computer forensic analysis. Further joint corroboration matching these details with artifacts retrieved from computers in industrial networks could present an opportunity to expand research into these campaigns.

Portable executable file infectors... everywhere

Providing a definition for portable executable (PE) infectors would likely be unnecessary for security professionals reading this paper from an IT perspective. However, as surprising as it sounds, this concept is only mildly recognized as it pertains to its relationship with OT security. In 2019 we developed a brief experiment hunting for samples of files related to seven major OT OEMs uploaded to online malware analysis sandboxes. While we have not publicly released this research, our results suggest that at least hundreds, if not thousands of OT-related PE binaries are infected each year by some of the most common malware strains.

At first glance, PE infectors do not appear to be problematic as they are often detected by basic anti-virus (AV) software. However, the unique circumstances of OT environments make it difficult to evaluate all of these samples using AV products and minor infections may result in serious performance implications for legacy OT systems. Besides, the implications of PE infectors reaching OT networks suggest that more complex malware is likely to do the same. The abundance of PE infectors included in OT-related samples is only one of many examples of problems that may be deemed simple from an IT perspective, but may be more problematic in the OT context. Collaboration between the two disciplines is again the best way to address this challenge given the limitations present in OT environments.

Internet-connected assets

Lastly, another incident registered in the OT-CSIO refers to financially motivated actors inadvertently accessing an Internet-connected HMI for air quality compliance. The incident was likely untargeted and resulted from searching for point-of-sale (POS) systems leveraging vulnerable services running on the remote desktop protocol (RDP) and virtual network computing (VNC) ports.

While the incident did not result in any negative impact, it highlights the challenges we face to secure Internet-connected equipment associated with physical processes. Any OT equipment that is connected to the Internet risks being compromised by highly skilled actors taking advantage of low-hanging fruit, moderately skilled actors engaging in opportunistic disruptions, or even low skilled actors exploring their capabilities. In fact, finding these types of exposed assets is fairly

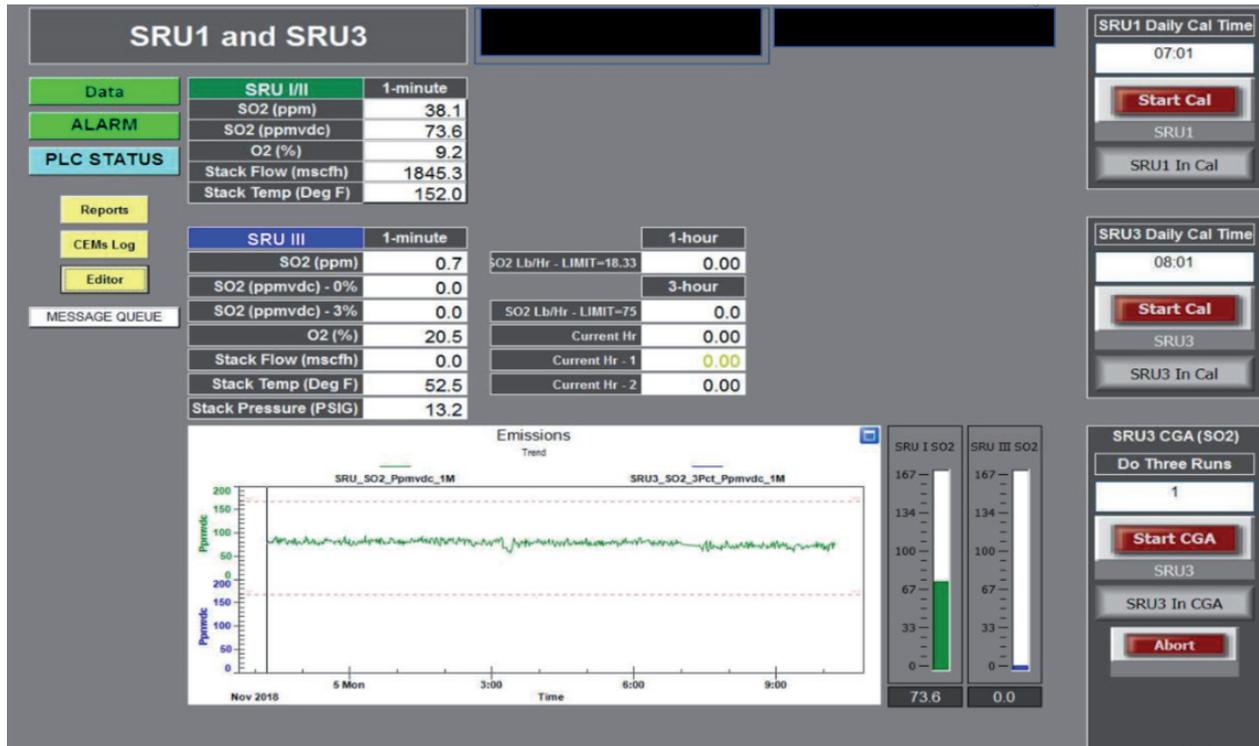


Figure 4: Example of inadvertently accessed Internet-connected HMI.

simple and can be achieved with mainstream open-source tools such as Shodan or Censys [2]. Although it is always recommended not to expose OT assets online, organizations continue to do so to benefit from remote accessibility to critical processes. Taking this into consideration, it is our challenge to identify mechanisms to secure these assets that are currently located at the lowest level of the security food chain.

IT IS NO SECRET THAT BOTH OF US ARE RUNNING OUT OF TIME

The cases described in this paper are some of many examples that illustrate the need for tighter collaboration between IT and OT security professionals to protect our most critical cyber physical assets. Although we still see a large disconnect between the two communities, we thought this was a unique opportunity to say, 'hello from the OT side'. It is time to evolve this narrative and start discussing how we can mix the two unique perspectives on security to reach common security goals. It is only by combining a deep understanding of both computing equipment and process automation that we will be prepared to respond to the increasingly complex threat landscape.

The book of OT security is still being written, with a myriad of challenges to solve. We cannot afford to learn from mistakes as successful cyber physical attacks may result in enormous damage to infrastructure, processes, and most importantly, people. As a result, those who decide to become truly engaged in solving these challenges are likely to become essential players in the cybersecurity field throughout the next decade.

REFERENCES

- [1] Fluchs, S. Why OT has different needs than IT. 01 March 2020. <https://medium.com/@fluchsfriktion/why-ot-has-different-needs-than-it-18ba9baa36e7>.
- [2] Kapellmann Zafra, D. VB2019 paper: Fantastic Information and Where to Find it: A guidebook to open-source OT reconnaissance. October 2019. <https://www.virusbulletin.com/virusbulletin/2019/11/vb2019-paper-fantastic-information-and-where-find-it-guidebook-open-source-ot-reconnaissance/#ref2>.
- [3] Ansari, K. Clean Up Your MES: The Bridge Between IT & OT. 2020. <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1583176005.pdf>.
- [4] Kapellmann Zafra, D.; Brubaker, N. The FireEye OT-CSIO: An Ontology to Understand, Cross-Compare, and Assess Operational Technology Cyber Security Incidents. 30 September 2019. <https://www.fireeye.com/blog/threat-research/2019/09/ontology-understand-assess-operational-technology-cyber-incidents.html>.
- [5] Ackerman, P. Industrial Cybersecurity. Packt, October 2017. https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch011v11sec10/the-purdue-model-for-industrial-control-systems.

- [6] Greenberg, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. 22 August 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
- [7] Kapellmann Zafra, D.; Lunden, K.; Brubaker, N.; Kennelly, J. Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT. 24 February 2020. <https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html>.
- [8] Abrams, L. SNAKE Ransomware Is the Next Threat Targeting Business Networks. 08 January 2020. <https://www.bleepingcomputer.com/news/security/snake-ransomware-is-the-next-threat-targeting-business-networks/>.
- [9] Cisomag. Attackers Target Industrial Control Systems with EKANS Ransomware. 05 February 2020. <https://www.cisomag.com/attackers-target-industrial-control-systems-with-ekans-ransomware/>.
- [10] Johnson, B.; Caban, D.; Krotofil, M.; Scali, D.; Brubaker, N.; Glycer, C. Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure. 14 December 2017. <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>.
- [11] FireEye Intelligence. TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. 23 October 2018. <https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html>.
- [12] Miller, S.; Brubaker, N.; Kapellmann Zafra, D.; Caban, D. TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping. 10 April 2019. <https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html>.
- [13] Cybersecurity Infrastructure Security Agency. Alert (TA18-074A)- Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. 16 March 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>.
- [14] Greenberg, A. A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems. 20 November 2019. <https://www.wired.com/story/iran-apt33-industrial-control-systems/>.
- [15] Legezo, D. WildPressure targets industrial-related entities in the Middle East. Kaspersky, 24 March 2020. <https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/>.