Targeting Control and Safety Instrumented Systems (SIS): new escalation of cyber threats to critical [energy] infrastructure

By Vytautas Butrimas*

"It is no use saying, 'We are doing our best.' You have got to succeed in doing what is necessary." – Winston Churchill[1]

Introduction

Industrial Control and Safety systems play an important part in insuring that the physical processes taking place in a manufacturing plant, power generation facility or other segment of critical infrastructure do not go out of preset parameters to damage expensive equipment, cause environmental harm or hurt people. However, if these systems fail or are made to fail a terrible price may be paid in terms of damaged property and even loss of life. If one thinks about driving an automobile down a highway at 100 km/hour the automobile's safety systems include the seat belts and breaks. If something were to happen to disable these two systems while driving down the highway nothing will immediately happen. However if there was an accident the failure of these disabled safety systems to perform their intended functions will lead to serious consequences for the car, driver and other innocent people involved in the accident.

This article will briefly review some past incidents that involved safety systems leading up to an analysis of the most recent incident of malware being used to intentionally disable a safety system in a petrochemical plant in 2017 and finish with recommendations and examples of lessons learned.

I. The importance of industrial control and safety systems has a long history of warnings

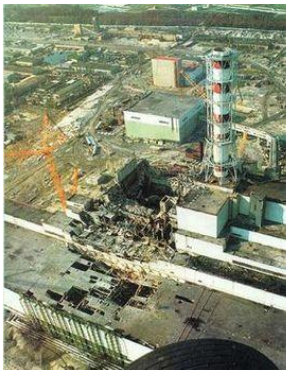
Once upon a time, there was a nuclear power plant located in a pleasant springtime countryside. The engineers of that plant wanted to perform a test of the reactor control systems under conditions of low power. They had tried the test a year earlier but the results were inconclusive. So after some equipment additions and modifications the engineers were ready to try the test again a year later. The engineers ran into some trouble in starting the test for some of the reactor safety systems would sound the alarm and fault causing the test to stop. So in order to achieve the conditions for the test the engineers disabled the troublesome safety system. The tests resumed but the system soon ran into serious trouble threatening to damage the reactor. Since the safety systems were disabled, there was no capability to stop events taking their course leading to a catastrophic reactor meltdown. This in short is the background to the events, which led to the Chernobyl nuclear disaster in 1986[2]. The nuclear power industry has moved on to see new improvements in ease of operations and safety. However, the importance of safety systems that designed to protect a critical

* Views and opinions expressed are those of author and do not represent the official view of any institution he is associated with.

[1] https://www.brainyquote.com/quotes/winston_churchill_100955

[2] Chernobyl Accident 1986 http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx

process from going out of control has increased over time together with advances in remote management capabilities and automation.



A dangerous experiment by poorly trained plant engineers which included disabling safety systems contributed to the cause of the Chernobyl disaster in 1986.

On June 10, 1999 an IT specialist was doing data development work using one of the computers connected to a real-time gasoline pipeline control and safety system in Bellingham, Washington. The extra work caused a problem with the transfer of pipeline sensor and other telemetry data to the controller. It failed silently without any alarms. The pipeline in the meantime ruptured and 237,000 gallons of gasoline poured into a creek. After 1.5 hours the controller knew nothing of this rupture since the flow of updated data had stopped leaving him to think that things were still normal when they were not. Then someone threw a match into the river, which ignited the gasoline killing 3 people and destroying a water plant that was located next to the river. The cost of the physical damage of this unintended accident reached 45 million USD and bankruptcy for the operator of the pipeline[3][4].

IT failure in critical infrastructure can have physical consequences. Bellingham, Washington on June 10, 1999 after 237,000 gallons of gasoline flowed into a river from a pipeline rupture.

[3] Board Meeting of National Transportation Safety Board, Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999 https://www.ntsb.gov/news/events/Pages/Pipeline_Rupture_and_Subsequent_Fire_in_Bellingham_Washington_June_10_1999.aspx 10/8/2002

[4] Full NTSB report: June 10, 1999 Pipeline Accident Report Pipeline Rupture and Subsequent Fire in Bellingham, Washington , NTSB/PAR-02/02 PB2002-916502, Adopted October 8, 2002 https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf

In 2007 the US Idaho National Laboratories conducted the "Aurora" vulnerability experiment to see if a cyber-attack could damage or destroy industrial equipment. In this case a diesel powered generator was set up in a test facility constructed to simulate a power grid. An "Aurora event consists of the out-of-sync reconnecting of three-phase rotating equipment. Three-phase equipment includes not only generators but also synchronous induction motors. This means that customer loads in manufacturing facilities, pipelines, refineries, electrified mass transit, and even data centers and power plants are directly at risk from Aurora"[5].

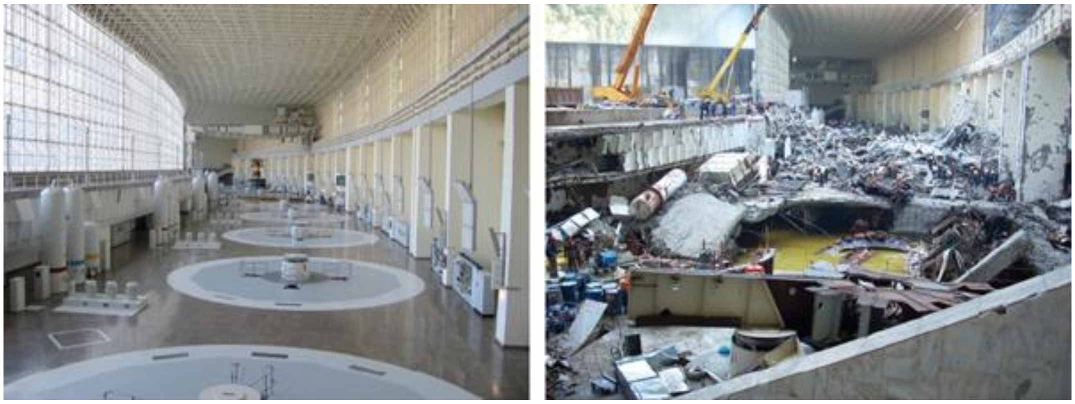
To this day the Aurora vulnerability effects electricity systems worldwide and potentially any rotating equipment. The key word here is "vulnerability". It is not a design flaw or something caused by a software bug – it is an issue of engineering under the laws of physics. However these laws can be manipulated using cyber means to cause damage and harm to people.

The "Aurora" experiment as reported by CNN which ended with destruction of a multi-ton electric power generator. It didn't happen because of security flaw or software bug, it was a fact of engineering and laws of physics that were manipulated to "brick" a multi-ton power generator (watch the experiment here https://www.youtube.com/watch?v=fJyWngDco3g).

On August 17, 2009 the world's 6th largest hydroelectric power producing complex at Sayano-Shushenskaya in Siberia suffered a control and safety system failure resulting in the loss of 75 skilled plant personnel, loss of most of the dam's 10 turbines and tons of oil flooding into the Yensei river. The official cause blamed loose turbine anchor bolts and poor management practices. However, the investigation also revealed a history of poor maintenance practices and a tendency to put economics of power production first before safety. Safety became a lower priority after the

[5] Swearingen, M., Brunasso,S. Weiss,Huber, D., What You Need to Know (and Don't) About the AURORA Vulnerability, Powermag http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?printmode=1 09/01/2013.

need to fill in a gap in power production from another plant that went off the grid. A turbine was allowed to operate at 4 times above the allowable vibration levels and the warnings of a recently installed but not accredited safety system were ignored. This resulted in a 1500 ton turbine rising 15 meters into the air and crashing into other turbines and equipment at the plant causing catastrophic damage requiring years to repair and great cost[6].



Before and after pictures of the turbine gallery at Sayano Shushenskaya Hydro Power Plant where 75 plant engineers were killed. Putting priorities of electric power economics over the warnings of safety systems contributed to this disaster.

Stuxnet malware discovered in 2010 intentionally disables safety systems

Up to now the events described have been accidental or unintentional with blame for disastrous malfunctions of industrial control systems being laid on incompetent or poorly thought out managerial and engineering decisions. In 2010 we learned of a new emerging threat with the appearance of an intentional effort to disrupt a safety system in order to produce damage to equipment used in a nuclear enrichment facility. There is still much to learn from a study of this cyber weapon developed by a state called Stuxnet. However by 2010 we learned of a demonstrated capability to neutralize a system used to insure the control and safety of a critical process. This cyber-attack was a focused attempt by a nation state or states at disrupting the production at a nuclear enrichment facility in a Middle Eastern country[7].

August 2017 Hatman/Triton malware causes shutdown of petrochemical plant

Stuxnet’s apparent success attracted significant attention and the methods demonstrated have continued to be developed. In December 2017 reports came from the US Government[8], private security companies and security journals about a cyber-attack targeting the control and safety instrumented systems (SIS) of a petrochemical plant located in the Middle East[9]. The malware known variously as Hatman, Triton or

[6] Boyko, A., Popov, S, Krajisnk, N., Investigating the Sayano Shushenskaya Hydro Power Plant Disaster, http://www.powermag.com/investigating-the-sayano-shushenskaya-hydro-power-plant-disaster/?printmode=1 12/01/2010

[7] Butrimas, V., International implications of securing our SCADA/control system environments, Handbook of SCADA/Control Systems Security 2nd Ed. Edited by Radvanofsky R., Brodsky J., CRC Press 2016 pp. 82-104.

[8] MALWARE ANALYSIS REPORT MAR-17-352-01 HATMAN—SAFETY SYSTEM TARGETED MALWARE https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf December 18, 2017

[9] Kovacs, E., New Triton ICS Malware Used in Critical Infrastructure Attack

Trisis was a specifically targeted remote access Trojan (RAT) designed to take over the safety controllers of a 16-year-old safety system manufactured by Schneider Electric[10]. Hatman is mentioned together with Stuxnet as it bears many similarities. For one it checks to see at several levels whether it is present on the targeted equipment. If it determines it is not where it is supposed to be it disables and deletes itself from memory. Hatman also shares Stuxnet's tailor made nature of malware made to fit the targeted system. All these common attributes also indicated the work of team of highly skilled programmers and engineers, use of intelligence gathering assets and the building of a testing laboratory. The attack on the control systems of the petrochemical facility was well underway and progressed to the point of delivering the executable payload to the safety system when something went wrong. Luckily for the plant operators, who up till now had no indication that their systems were compromised, the attackers made a mistake in the code. It appears that the attackers made a mistake and did not remove all the bugs in their attack software [11]. The safety systems sensed something wrong and safely shut down the plant. It is interesting to note that the operators only knew something was wrong after the shutdown. They had no idea that their critical systems were compromised. This was a "close call" where tragedy was avoided by the sloppy programming of the attackers and by the plants staff that had the curiosity and capability to look into why the plant shutdown.

II. The importance of control and safety systems and implications of becoming targets for cyber-attacks

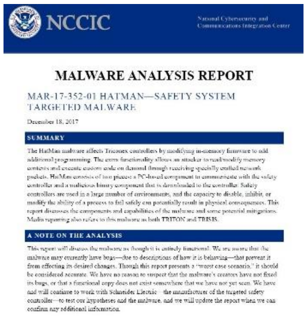
What is the significance of the Hatman malware attack on industrial control and safety systems? At the very least it shows that disabling systems used to watch over a critical process is still of interest to those developing cyber-attacks. On the other hand, the focus on compromising and taking over the control of a safety system also represents a serious escalation of the cyber threat to critical infrastructure. Control and safety systems are used in an industrial process to protect property and most importantly, people from serious harm resulting from an industrial process that has gone outside of set parameters. These parameters are used to program an automatic response to bring a system back to a safe state when changes for example in temperature, flow rates, pressure, frequency or other system state indicators exceed preset levels. These are the systems that automatically respond to open or close valves on a gas pipeline when pressures or flow rates go beyond preset parameters. These are the systems that automatically shutdown a nuclear reactor when something goes wrong with the cooling and pumping systems. If something is done to intentionally neutralize the functions of these systems serious harm can result if a system state exceeds set parameters. It is like disabling the breaks and seat belts without the knowledge of the driver. Nothing immediately bad will happen to the driver of the car but if there was a sudden need to stop the consequences could be most serious. In other words safety systems are the last line of defense provided by automated technologies to save us from having to deal with something "going boom in the night". This emerging danger represents a far different kind of cyber threat that most IT specialists are familiar with. It has nothing to do with stealing of data in a document, nothing to do with dealing with a web defacement or a denial of service attack. These IT events are recoverable with no harm done to the human being or the environment. In most cases the reboot of the troubled computer or installation of a software update will be enough to bring the IT system back to normal. In the case of an intentional compromise of a control or safety system in an

http://www.securityweek.com/new-ics-malware-triton-used-critical-infrastructure-attack December 14, 2017

[10] Forney, P., King, A. S4 Conference video presentation on "TRITON - Schneider Electric Analysis and Disclosure" , https://www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be

[11] Perlroth, N., Krauss, C., A Cyberattack in Saudi Arabia Had a Deadly Goal Experts Fear Another Try https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html March 15, 2018.

industrial environment of operational technology (OT) recovery is counted in terms of costs for replacing damaged equipment, damaged property and loss of human life.



NCCIC National Cybersecurity and Communications Integration Center

MALWARE ANALYSIS REPORT

MAR-17-352-01 HATMAN—SAFETY SYSTEM TARGETED MALWARE

December 18, 2017

SUMMARY

The HatMan malware affects Triconex controllers by modifying in-memory firmware to add additional programming. The extra functionality allows an attacker to read/modify memory contents and execute custom code on demand through receiving specially crafted network packets. HatMan consists of two pieces: a PC-based component to communicate with the safety controller and a malicious binary component that is downloaded to the controller. Safety controllers are used in a large number of environments, and the capacity to disable, inhibit, or modify the ability of a process to fail safely can potentially result in physical consequences. This report discusses the components and capabilities of the malware and some potential mitigations. Media reporting also refers to this malware as both TRITON and TRISIS.

A NOTE ON THE ANALYSIS

This report will discuss the malware as though it is entirely functional. We are aware that the malware may currently have bugs—due to descriptions of how it is behaving—that prevent it from effecting its desired changes. Though this report presents a "worst case scenario," it should be considered accurate. We have no reason to suspect that the malware's creators have not fixed its bugs, or that a functional copy does not exist somewhere that we have not yet seen. We have and will continue to work with Schneider Electric—the manufacturer of the targeted safety controller—to test our hypotheses and the malware, and we will update the report when we can confirm any additional information.

Reports and analysis of Hatman came out in December of 2017 yet this information has not found itself in some later summary reports about cyber threats nor led to changes in policies. Is this due to a lack of imagination, fear of "thinking out of the box" or thinking that "this happened there but it can't happen here"?

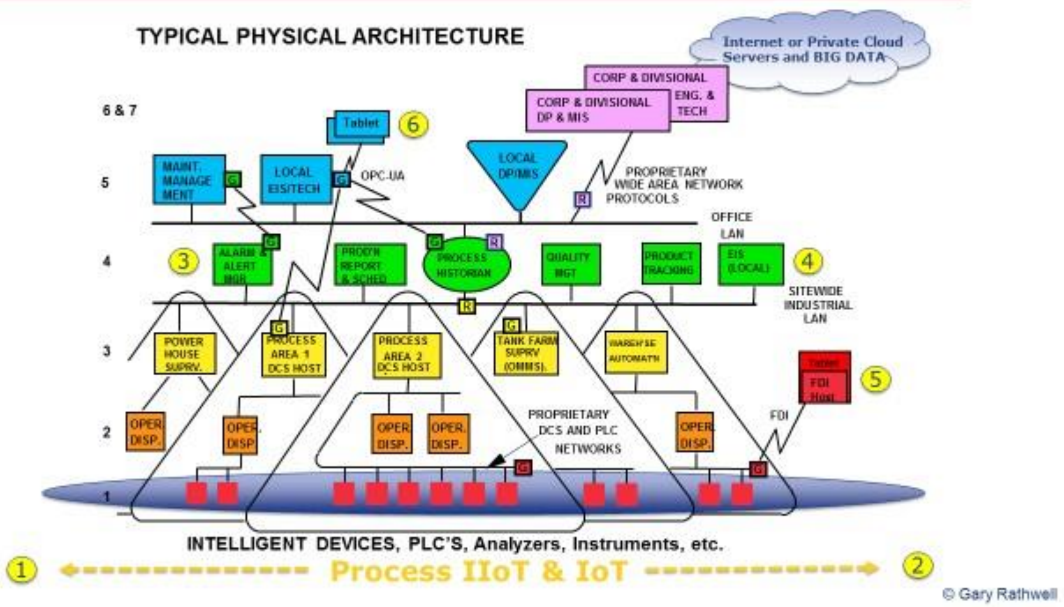
Some good efforts underway to address the problem but others still have a long way to go.

There is perhaps a good outcome to the Hatman story. It has attracted the attention of industry, manufacturers and the engineers who work for them. Soon after the Hatman story broke, two workgroups were created to deal with the problem of poor cybersecurity on industrial devices. The International Society for Automation's Committee on Industrial Automation and Control Systems Security (ISA 99)[12] created a subgroup (WG4 TC7) to come up with recommendations for dealing with the lack of cybersecurity found in Level 0 and 1 industrial devices of the Purdue Model[13]. These are the devices that are closest to the physical process such as actuators, sensors, program logic controllers and safety devices. It is the objective of this group (which includes the participation of manufacturers and the engineers) to provide cybersecurity guidance to insure the safety and reliability of those devices already installed in the field and to guide the secure design of new devices.

[12] https://www.isa.org/isa99/

[13] Purdue Reference Model for CIM http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html

How Does this Fit in Control & Information Systems?



© Gary Rathwell

See the control system architecture graphic above. ***There is a lack of security in those devices that are closest to the physical process of an industrial operation*** *(found at the bottom of this graphic at Level 1 and below at "0" or IIoT /IoT level)) Most of the efforts at improving IT security deal with protecting the "information" on the network and are focused at the upper levels (4,5,6,7). A study of the bottom part revealed significant security gaps. There the protection of the physical process is most important,whether a malicious actor could gain access to the device to compromise its integrity and use it to damage equipment.* ***Graphic shown with the permission of Mr. Gary Rathwell, President, Enterprise Consultants.***

Next, an institution of the European Union took the initiative to create a workgroup to also deal in part with the issues raised by Hatman. The Industry 4.0[14] Cybersecurity Experts Group (EISA) created in early 2017 by the European Union's ENISA[15] "aims at gathering experts at the crossroads of industrial systems and Internet of Things (IoT)[16] to exchange viewpoints and ideas on cyber security threats, challenges and solutions." As with the ISA group the EISA group also includes representatives from manufactures and policy makers[17].

Work groups like these really have a problem on their hands. How to provide relevant guidance for the massive implementation of increasingly connected devices and sensors in a safe way. The recognition of the need to address the security of these devices has unfortunately come after the installation of millions of connected devices. The challenge to keep track of where these devices are and what they are connected to is awesome. It is very difficult to believe anymore in a plant manager or CEO of a company when they

[14] In North America this is also known as the Internet of Things (IoT) or the Industrial IoT (IIoT)

[15] https://resilience.enisa.europa.eu/eics-experts-group

[16] ENISA defines the IoT as "an emerging concept describing a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. Internet of Things is tightly bound to cyber-physical systems and in this respect is an enabler of Smart Infrastructures by enhancing their quality of service provisioning." https://resilience.enisa.europa.eu/eics-experts-group

[17] List of EISC work group members and the manufacturers represented: https://resilience.enisa.europa.eu/eics-experts-group/members

say that “our critical systems are safe from cyber-attack since they are not connected to the Internet”. One manager found this out when his enterprise’s sensitive database was breached from just one connected sensor functioning as an IoT device. In this case, it was a thermometer in the aquarium located in the lobby of his company![18] Wonder if the fish survived the attack?

Lessons learned

There are some lessons to learn from this discussion of a just a sample of the publically known unintended failures and intentional attacks on industrial systems used for control and safety:

1. A false sense of security can arise in thinking that one’s critical systems are safe if they are not connected to the Internet. Insuring complete isolation from the Internet can perhaps be still achieved by placing a device in the middle of the Sahara Dessert. Even that may not work since we learned that the nuclear enrichment facility that was attacked by the Stuxnet malware was located 50 feet under the dessert and still the malware somehow found its way there. Industrial systems are so complex and as the Industry 4.0 movement with its array of connected IoT and IIoT devices progresses it will be increasingly hard to keep track of all the devices and processes to make sure there is no contact with the Internet. There is also the very real possibility that the compromise will originate from inside the network. An engineer might open a connection during the weekend so he could access some process he is concerned about from his home. A vender arriving at a site to perform maintenance work could transfer an infection to the air-gapped plant with his infected notebook computer. There are industrial sites that for convenience purposes (don’t’ want to send an engineer out to a remote site during the middle of the night) use wireless technologies to communicate with remote field equipment. To paraphrase the artist Andy Warhol, someday every thing in the world will be connected to the Internet for 15 minutes. This is not hard to imagine when refrigerators, stoves, and home thermostats are being given IP addresses and can be accessed over a mobile phone.
2. In addition to the operators of critical infrastructure assigned with watching over the day-to-day operations of an industrial process a new section needs to be created with the task of monitoring and reacting to malicious or unintentional changes in process flows, equipment performance and data flows that go beyond expected norms. Namely an Industrial Security Operations Center (ISOC). The intent would be to establish a monitoring capability that could detect a malicious intrusion within 24 hours. It is not enough to look after the cybersecurity of the business side of the facility, the cybersecurity needs of the operations on the plant floor also need addressing;
3. The operator of a pipeline, power generation and distribution facility, water utility or any larger manufacturing enterprise needs to engage in a dialogue with their equipment vendor about security. Operators for example need to ask the vendor about the manufacturers security practices (is the customer notified when software patching is performed, are there any “backdoors” placed by the manufacturer on the equipment that allow outside access to the equipment?). A good example is Schneider Electric’s openness about the Hatman malware and disclosing what they knew at a recent security conference [19].
4. Think first whether a new IT feature is needed for the new equipment. Not all of the new functionalities and connectivity options offered as “selling features” by manufacturers are needed

[18] Williams-Grutt, O., “Hackers once stole a casino’s high roller database through a thermometer in the lobby fish tank” http://www.businessinsider.de/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?r=UK&IR=T Business Insider Deutschland 2018-04-15

[19] TRITON - Schneider Electric Analysis and Disclosure , video presentation, https://www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be , S4 Events 2018

(for example adding an IP address to an aquarium thermometer or thermocouple[20]). At the least, the manufacturer should explain what the new features are and how to disable them if not needed.

5. The tendency to integrate safety, control and business networks into one network in spite of the advantages in lower overhead and savings is to be resisted and if implemented, wisely managed[21]. Think twice before jumping into the Industry 4.0[22] movement. There are important security and cost caveats to consider[23] first before one can safely implement these new and promising technologies in an industrial environment.
6. The active participation of states in these incidents is most disturbing as there has been no counterweight to manage and control this behavior from the international security policy making community. The apparent freedom to act has encouraged the belief that this kind of activity is effective, cheap and deniable.

A step in the right direction. Schneider Electric engineers share analysis and recommendations on Hatman at industry conference S4 in Miami. Example of prompt and informative industry public disclosure about an incident involving their products [24].

Conclusions

As we enter this darker period in the history of cyberspace and understand the new threats to critical infrastructure, it is evident that some Government institutions and those tasked with protecting our critical infrastructure from cyber intrusions and attacks remain poorly informed or lacking in curiosity. The government of the Australian province of Northern Territory recently announced the allocation of significant funds to establish a cybersecurity center[25]. It is intended to become "the central base for cyber analysts, engineers and forensic specialist staff to monitor, identity and respond to malicious cyber-attack

[20] 1732E ArmorBlock Dual-Port EtherNet/IP 4-Point Thermocouple and
RTD Input Modules http://literature.rockwellautomation.com/idc/groups/literature/documents/in/1732e-in005_-en-e.pdf

[21] Here is one manufacturer proposing to do just that by integrating safety systems. Selega, R., "How to remain safe and profitable during Industry 4.0" https://www.abb-conversations.com/2018/01/how-to-remain-safe-and-profitable-during-industry-4-0/ ABB January23, 2018

[22] https://en.wikipedia.org/wiki/Industry_4.0

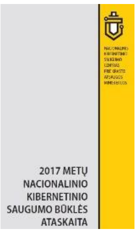
[23] Watch "Brave New Industrie 4.0" presented by the man who analyzed Stuxnet, Mr. Ralph Langner. https://www.youtube.com/watch?v=ZrZKiy2KPCM

[24] Video of presentation at S4 https://www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be

[25] https://www.itnews.com.au/news/nt-govt-to-build-cyber-security-operations-centre-489049?eid=3&edate=20180416&utm_source=20180416_PM&utm_medium=newsletter&utm_campaign=daily_newsletter

or intrusions on government IT systems."[26] It is not clear if this new center will be capable to deal with the effects of a failure to the power grid from a cyber-attack since there is no mention of critical infrastructure protection as a responsibility of this new center. The main identified threat seems to be cybercrime while the threat from state sponsored attacks on critical infrastructure like Hatman go unnoticed for officials responsible for governing this Australian province.

To take a look for comparison on the other side of the world in Lithuania a similar limited mindset seems also present. The National Cybersecurity Center of Lithuania under the Ministry of National Defence issued its National Cybersecurity Report for 2017 (2017 Metų Nacionalinio kibernetinio saugumo būkles ataskaita)[27] presented to the public in March 2017. According to the Law on Cybersecurity the Center is also tasked to look after Lithuania's "Critical Information Infrastructure". For a report that claims to cover all of the significant cyber events of 2017 it is remarkable that the list of dangerous malware stops during the summer of 2017 with mention of the WannaCry and NotPetya ransomware. It is strange that these two examples while considered serious were not analyzed further since these threats did not materialize or cause any damage in Lithuania.[28] NotPetya was apparently targeted at Ukraine but the "collateral damage" was found outside of Ukraine as experienced by multinational corporations such as shipping company Maersk[29]. One senses an avoidance of any desire to do any "thinking out of the box" and a lack of imagination on the part of the authors of the report. There were far worse cases of malware that were discovered in the Fall and Winter of 2017 which one would think deserved mention in the report. For example, CrashOveride/Industroyer was reported as being a cyber-attack platform specifically designed to attack and disrupt electric grid control systems [30]. I have already mentioned the reports of the Hatman/Triton/Trisis malware attack on a Middle Eastern petrochemical facility. The attack was discovered in August of 2017 and public reports were available since December. Raising awareness and taking a wider look at the threat environment presents to all of us a challenge.



2017 METŲ
NACIONALINIO
KIBERNETINIO
SAUGUMO BŪKLĖS
ATASKAITA

Not all institutions responsible for national cybersecurity look at the cyber threats in the same way. This report on cybersecurity for 2017 missed two important malware events that could affect critical infrastructure. We must face the challenge to "think out of the box" and not be afraid of what we may find out, even though it may add to the work of insuring the security of a nation's critical infrastructure.

The last point to make before closing is that the reports of malware targeting industrial control and safety systems in 2017 focused on equipment manufactured by well-known western brand names. The attackers may have targeted equipment located in Ukraine and in the Middle East **but since the same equipment is used by other operators the methods can be applied anywhere in the world**. Most importantly, the

[26] Ibid.
[27] https://www.nksc.lt/doc/NKSC_ataskaita_2017_%5blt%5d.pdf
[28] Ibid. p. 2
[29] Greenberg, A., The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, August 22, 2018 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ .
[30] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf

perpetrators are getting a lot of practice at disrupting the technologies we all depend on and are getting to be good at what they are doing.

It does not appear that the defenders are going to be a match for these attackers if the current limited thinking about cyber threats continues. This is an issue that cannot be left to the engineers and private sector to solve alone. Governments together with their international partners in security policy making and law enforcement need to get serious about developing norms for managing the malicious state behavior in cyberspace. The appearance of advanced and persistent malicious cyber capabilities together with the willingness to use them without apparent concern for the consequences, pose serious threats to securing the daily activities found in the modern economy, national security and well-being of society. The appropriate conclusions need to be made and appropriate steps taken to address and manage these new threats from cyberspace

Vilnius, 2018-08-28

Footnotes

1. https://www.brainyquote.com/quotes/winston_churchill_100955

2. Chernobyl Accident 1986 http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx

3. Board Meeting of National Transportation Safety Board, Pipeline Rupture and Subsequent Fire in Bellingham,Washington, June 10, 1999 https://www.ntsb.gov/news/events/Pages/Pipeline_Rupture_and_Subsequent_Fire_in_Bellingham_Washington_June_10_1999.aspx 10/8/2002

4. Full NTSB report: June 10, 1999 Pipeline Accident Report Pipeline Rupture and Subsequent Fire in Bellingham, Washington , NTSB/PAR-02/02 PB2002-916502, Adopted October 8, 2002 https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf

5. Swearingen, M., Brunasso,S. Weiss,Huber, D., What You Need to Know (and Don't) About the AURORA Vulnerability, Powermag http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?printmode=1 09/01/2013.

6. Boyko, A., Popov, S, Krajisnk, N., Investigating the Sayano Shushenskaya Hydro Power Plant Disaster, http://www.powermag.com/investigating-the-sayano-shushenskaya-hydro-power-plant-disaster/?printmode=1 12/01/2010

7. Butrimas, V., International implications of securing our SCADA/control system environments, Handbook of SCADA/Control Systems Security 2nd Ed. Edited by Radvanofsky R., Brodsky J., CRC Press 2016 pp. 82-104.

8. MALWARE ANALYSIS REPORT MAR-17-352-01 HATMAN—SAFETY SYSTEM TARGETED MALWARE https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf December 18, 2017

9. Kovacs, E., New Triton ICS Malware Used in Critical Infrastructure Attack December 14, 2017, http://www.securityweek.com/new-ics-malware-triton-used-critical-infrastructure-attack

10. Forney, P., King, A. S4 Conference video presentation on "TRITON - Schneider Electric Analysis and Disclosure" , https://www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be

11. Perlroth, N., Krauss, C., A Cyberattack in Saudi Arabia Had a Deadly Goal Experts Fear Another Try, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html March 15, 2018.

12. https://www.isa.org/isa99/

13. Purdue Reference Model for CIM http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html

14. In North America this is also known as the Internet of Things (IoT) or the Industrial IoT (IIoT)

15. https://resilience.enisa.europa.eu/eics-experts-group

16. ENISA defines the IoT as "an emerging concept describing a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. Internet of Things is tightly bound to cyber-physical systems and in this respect is an enabler of Smart Infrastructures by enhancing their quality of service provisioning." https://resilience.enisa.europa.eu/eics-experts-group

17. List of EISC work group members and the manufacturers represented: https://resilience.enisa.europa.eu/eics-experts-group/members

18. Williams-Grutt, O., “Hackers once stole a casino’s high roller database through a thermometer in the lobby fish tank” http://www.businessinsider.de/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?r=UK&IR=T Business Insider Deutschland 2018-04-15

19. TRITON - Schneider Electric Analysis and Disclosure , video presentation, https://www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be , S4 Events 2018

20. 1732E ArmorBlock Dual-Port EtherNet/IP 4-Point Thermocouple and RTD Input Modules http://literature.rockwellautomation.com/idc/groups/literature/documents/in/1732e-in005_-en-e.pdf

21. Here is one manufacturer proposing to do just that by integrating safety systems. Selega, R., “How to remain safe and profitable during Industry 4.0” https://www.abb-conversations.com/2018/01/how-to-remain-safe-and-profitable-during-industry-4-0/ ABB January23, 2018

22. https://en.wikipedia.org/wiki/Industry_4.0

23. Watch “Brave New Industrie 4.0” presented by the man who analyzed Stuxnet, Mr. Ralph Langner. https://www.youtube.com/watch?v=ZrZKiy2KPCM

24. Video of presentation at S4 https://www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be

25. https://www.itnews.com.au/news/nt-govt-to-build-cyber-security-operations-centre-489049?eid=3&edate=20180416&utm_source=20180416_PM&utm_medium=newsletter&utm_campaign=daily_newsletter

26. Ibid.

27. https://www.nksc.lt/doc/NKSC_ataskaita_2017_%5blt%5d.pdf

28. Ibid. p. 2

29. Greenberg, A., The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, August 22, 2018 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

30. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf