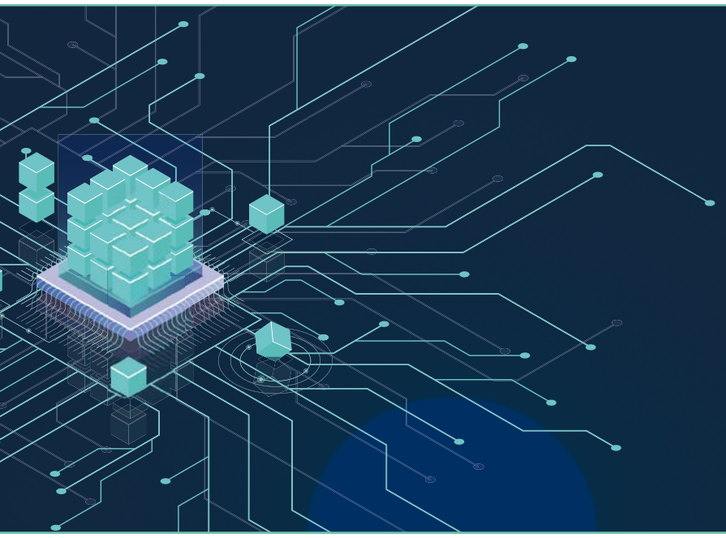


Report on Cyber Threats to Operational Technologies in the Energy Sector

GE Steam Power
Brown-Boveri-Strasse 7
Baden AG
5400, Switzerland

Tour Carpe Diem
31 place des Corolles
92098 Paris La Défense

> thalesgroup.com <

JANUARY 2020

contents

Illustration table

Foreword

Understanding the cyber threats to industrial facilities has become essential as the cyber ecosystem is proving so successful in its ability to defeat them. It is from this joint observation by Thales and General Electric that the willingness to think together, in the framework of their global agreement, about the relevant means that can be put at the service of organizations to defend themselves was born. With proven experience in the field of cyber threat analysis and treatment and the understanding of industrial security systems in the energy sector, Thales and General Electric have chosen to combine their joint expertise to shed some light on these threats. From the smallest building block of industrial control systems to the heart of these essential systems themselves, via the supply chain of organizations and the interfacing of their IT and OT systems, the combined expertise of Thales and GE makes it possible, through this report, to consider not only the degree of threat to the sector but also the conjunctural and structural vulnerabilities that can facilitate the task of attackers.

This report therefore takes the form of a handbook allowing each organization to integrate the best practices to follow and the threats to be taken into account to ensure effective cyber defense.

This in-depth analysis offered to the industry proves that only the synergy of expertise can provide sufficient knowledge to think about cyber defense. We hope that this document, which we wanted to be particularly rich and detailed, will be of great use to all stakeholders in the energy sector, and beyond that, to all economic players, so that they can better understand and therefore better combat this phenomenon they are facing, with potentially very high levels of damage. This analysis, which is not confined to mere conjecture, offers a series of strategic and operational recommendations based in particular on the good practices enacted by the ANSSI.

We wish you an enriching and pleasant reading.

Pierre JEANNE
Thales
Vice – President
System Security Division

Olivier JAMART
General Electric
General Manager
GE Steam Power Automation and Controls

Executive Summary

The report on cyber threats to industrial security systems from Thales and General Electric's is an original proposal for an analysis of a subject often considered to be sufficiently documented.

The proven experience of Thales, in terms of Cyber Threat Intelligence, and General Electric, in terms of understanding critical infrastructures in the field of energy, offers an unprecedented analysis in terms of methodology about threats to this type of systems. Successful attacks like that of the ATK91 group (Xenotime), presented into the Cyber Threat Handbook[1], which had targeted the Triconex Industrial Control System of a Saudi petrochemical plant in 2017, demonstrate once again how decisive it becomes to think of a defense in depth of these systems.

This dual expertise provides a detailed understanding of the threat landscape in the sector and particularly the threats to critical energy infrastructure systems. Industrial security systems have obviously reached a good level of maturity in terms of cybersecurity. Nevertheless, the number of attacks on them is increasing. Ninety percent of attacks are relatively unsophisticated, but due to the specificity of OT systems, they can have massive consequences for the energy sector today. Solutions exist and are available, but the rigidity of these systems and the practices surrounding them mean that they are not implemented. As for the remaining ten percent of attacks, they correspond to high-performance state-sponsored attackers or high-flying cybercriminals, against whom generic solutions do not exist. These attacks require a high level of maturity, dedicated, and sophisticated remediation.

Added to this is the growing intertwining of companies' IT and OT systems, which allows attackers to create bridges between any machine and the core infrastructure. The evolution of the sector moving towards a confusion of these systems present in each company pushes us to redefine the difference between them to remind the good practices to be observed on a daily basis.

The report is also an opportunity to recall how agile and scalable the cyber-ecosystem is. The increase in Supply Chain attacks, the phenomenon of Malware-as-a-Service and the multiplication of design compromises should encourage manufacturers and institutions to constantly monitor the evolution of the threat in order to avoid becoming an easy victim.

The collaboration between Thales and GE makes it possible to apprehend classic and common attacks, but also to see the hidden side of the iceberg, to consider attacks that are rarely seen but whose potential destructive capacities for data and infrastructures are decisive.

Attacks on these systems by state-sponsored groups are, for example, quite rare. Nevertheless, geopolitical and strategic turpitudes may be sufficient reasons for some states and groups to launch targeted and destructive attacks on these systems. Such a case would obviously be dramatic since it would involve serious attacks on sensitive infrastructure such as petrochemical or nuclear power plants. This risk obviously remains low, since the takeover or attack on an energy infrastructure by a third State constitutes a declaration of war under international law. Nevertheless, some state-sponsored groups, such as ATK91 (Xenotime) presented in this report, continue to specialize in compromising specific protocols for certain ICS systems. This widespread phenomenon proves that some States, through groups they sponsor, do not exclude the possibility of harshly targeting these systems and infrastructure in the event of international conflicts.

Current geopolitical events, which we can see in particular between Iran and the United States, show that this risk cannot be ignored. An understanding of the cyber threat to industrial security systems in the energy sector cannot do without a more systemic analysis that takes into account the major geopolitical movements at work. Recent attacks and increasing global tensions are driving countries to increasingly enforce Cybersecurity on critical infrastructure. Companies need to comply to global standards like IEC 62443 and NERC CIP which is more and more enforced in national laws.

Considering the four possible attack scenarios:

- **Targeted and direct attack**
- **Targeted and indirect attack**
- **Direct non-targeted attack**
- **Indirect non-targeted attack**

Thales and GE have developed use cases, making it possible to envisage any type of attack, regardless of its scale or complexity.

This report is the result of a joint reflection between two leaders in the fields of information systems security and critical energy infrastructures and provides a relevant analysis of the threats to the critical systems of our industrial infrastructures. It is accompanied by a series of operational and strategic recommendations based on the good practices proposed by the ANSSI[2].

1 - https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who

2 - https://www.ssi.gouv.fr/uploads/IMG/pdf/Guide_securite_industrielle_Version_finale-2.pdf

Glossary

ANCS: Act on the National Cybersecurity System (Poland)

APT: Advanced Persistent Threat

CIS: Center of Internet Security

EPCIP: European Programme for Critical Infrastructure Protection

ICS: Industrial Control System

IT: Internet Technology

LPM: Loi de Programmation Militaire

NIPP: National Infrastructure Protection Plan

NIST: National Institute of Standards and Technology

OEM: Original Equipment Manufacturer

OT: Operational Technology

PPA: Power Purchase Agreement

LD: Liquidated Damages

SCADA: Supervisory Control and Data Acquisition

SME: Small Medium-sized Enterprise

1. INTRODUCTION

The cyber threat landscape is constantly changing. It confronts cyber-attackers of very different natures, ranging from Advanced Persistent Threats (APT), characteristic of state-sponsored attackers, carrying out geo-strategic attacks, cybercriminals of varying levels in search of financial gain, cyber-terrorists maintaining their proselytizing and destruction campaigns, hacktivists using digital space as a vehicle for disseminating their ideologies, and finally script kiddies, those attackers seeking recognition who act out of opportunism. These self-interests draw profiles that could be considered simple to understand by large organizations and institutions in the context of the analysis of the cyberthreat. However, in addition to this myriad of attackers, there is also a web of competing interests and events. International, ethnic, social and economic tensions drive the motivations of attackers and transform what might be considered a simple landscape into an incredibly complex cyber-ecosystem. No industry is spared, no country, no community and no individual.

This complexity is compounded by technological change, which is even more rapid than the evolution of the threat. The latter, due to a lack of time, means or effort, is not necessarily followed by the need for security on the part of organizations. Vulnerabilities on organizations' systems are multiplying. Organizations themselves are intertwining, developing their supply-chain and thus expanding the potentially vulnerable surface by constantly creating new entry points for attackers.

This set of dynamics makes the threat's ecosystem more alive than ever. New practices are constantly emerging. On the Dark and Deep-Web, the phenomenon of Malware-as-a-Service is developing. Platforms offer on a classic market model to buy and sell malware and tools to carry out cyber-attacks. These cyber threat agoras allow attackers to trade and help each other. The modes of attack thus tend to merge, as generic malware models are used by both script kiddies and the world's most successful cyber-attack groups. This ever-changing threat invests a great deal of effort in the need for concealment, making it more difficult to analyze and understand.

Nevertheless, cyber threat analysis can identify the relevant attackers for an organization, understand their modus operandi, know their arsenal and identify the vulnerabilities they use in systems with precision. It is through this effort that relevant cyber defence can be put in place. A well-focused cyber defence that does not involve a crippling cost, is not unnecessarily time-consuming, and can save an organization.

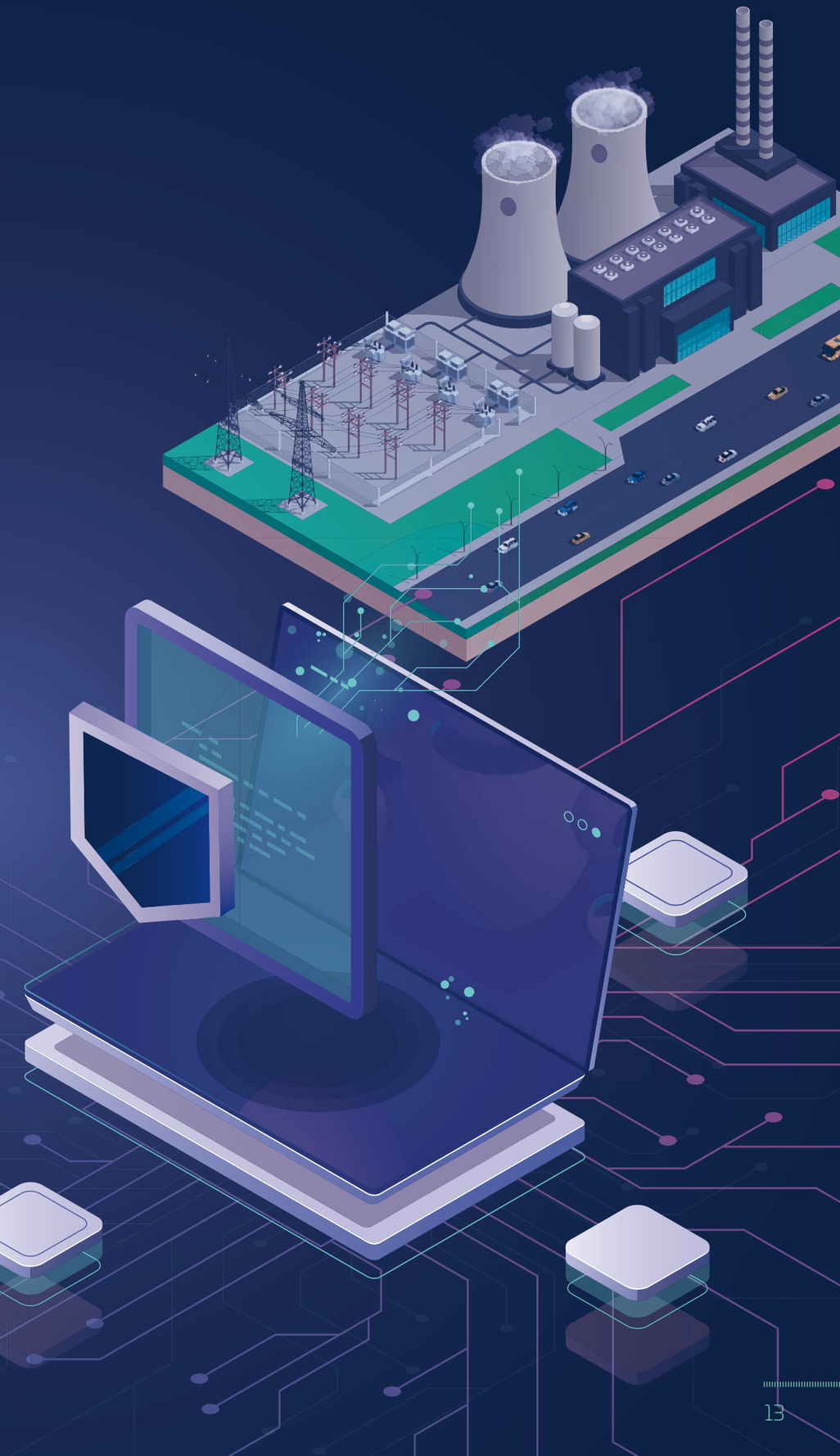
The purpose of this report is thus to diagnose the degree to which the cyberthreat to the energy sector, particularly to industrial control systems (ICS), has reached the point where a specialized analysis can lead to simple and effective solutions. After analyzing the threat landscape in the sector, the Thales and GE report addresses one of the most critical structural issues facing the sector given the nature of the threat in place. The report analyses the lack of understanding of the interrelationships between IT and OT systems and the related vulnerabilities, as well as the weaknesses specific to industrial control systems. While vulnerabilities in IT environments are mostly understood and managed. Vulnerabilities in OT / ICS environments still often lack attention. While systems are getting more and more connected (IoT) also vulnerabilities in non-connected OT environments get exploited. The different architectures, protocols, maintenance/ update cycles and the sensitive connection to OT Safety requirements requiring Cybersecurity solutions with OT deep domain expertise.

This double diagnosis, first of the threat and then of the vulnerabilities specific to industrial control systems, is accompanied by 4 case studies:

- The direct and targeted attack by ATK91 (Xenotime) on a Saudi petrochemical plant in 2017,
- The campaigns, which were not only aimed at the energy sector in particular, but which were turned directly on the OT systems of the targets by DrangonFly,
- The non-targeted attack by ATK88 (LockerGoga) which indirectly affected the OT system of the Norwegian company NorskHydro,
- The attack dedicated to the energy sector by the ATK6 (Energetic Bear) group indirectly through the suppliers of major industrialists in the sector.

These use cases make it possible to envisage every type of attack imaginable on these systems, whether or not they target the energy sector in particular, whether or not they are direct.

2.
CYBER THREAT IN THE POWER LANDSCAPE



2.1. A sector in transition

A sector in transition

The power sector is in transition. Global trends are creating an environment of disruption and driving the need for digital industrial software and services for the energy industry to become more efficient, reliable, secure, and sustainable.

Traditional and emerging, physical and digital, large and small, a mix of new technologies are converging to create a 21st-century power network, capable of realizing new and positive outcomes for people and the planet. GE is leading this transformation and co-creating the future of energy with our customers, providing safe, efficient, reliable, and affordable power to drive economic growth and raise living standards around the world.

Three main trends:

Decarbonization: Through Air Quality Control Systems, efficiency gains and a robust energy mix, the global power system can be a force for reducing CO2 and combatting climate change.

Digitalization: A new age of end-to-end integration with a single source of truth from edge to center is realizing unprecedented new outcomes for customers and the world.

Decentralization: Smaller, decentralized power systems are extending access and boosting resiliency in time to meet rising demand in burgeoning cities and remote areas.

The introduction and increasing penetration of renewables is changing the realities of the power market. Fossil fuels will have now a different, but still very important, role to play in the energy mix. As an example, in past years, coal plants were operating in baseload. Today, they are operating in more of a grid response function. Flexible coal power is required to provide available energy around the globe, and balance grids to support intermittent renewable energy.

Over the next 10 years, 25% of all future power capacity additions will be coal- or oil-fired steam power plants. And the installed capacity of nuclear power plants will increase by more than 140GW[3].

Nuclear power is the only large-scale dependable energy source producing no CO2 or other greenhouse gases, and will remain an integral part of the energy supply.

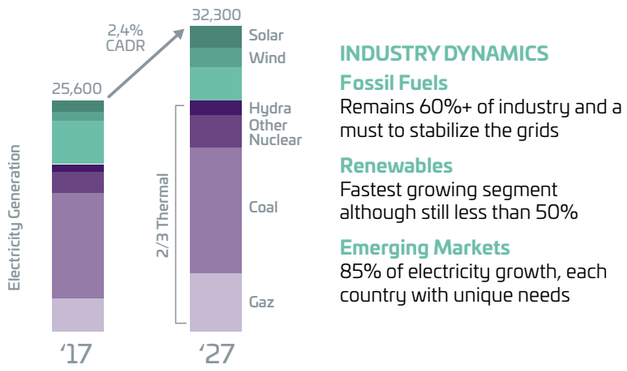
At the end of 2018, more than 456 commercial nuclear power reactors (>400 GW) were in operation, providing about 12 percent of the world's electricity. More than 140 GW of new capacity is foreseen by 2025.

These major trends are changing the electricity ecosystem from the production over the grid transmission to the end-user consumption. Old approaches and techniques are no longer viable; the industry is demanding new digital enablers and connectivity to enhance operating performance, increase flexibility and enable the transition of the energy mix.

Organizations in the sector are thus expanding their networks, making them more efficient and dedicated through increased digitization. The latter must be done in a reasonable way, which implies an extension and a strengthening of SCADA and ICS systems.

With the rise of new technologies (connected objects, advanced metering, storage batteries), individuals and SMEs (Small and medium-sized enterprises) will become an integral part in the energy ecosystem. Consumers will be able to obtain electricity in a short circuit or storage capacity and play a key role in controlling their consumption. The consequence will be the emergence of microgrids (decentralization), requiring even more flexible power supply and interconnectivity.

Global Power Outlook



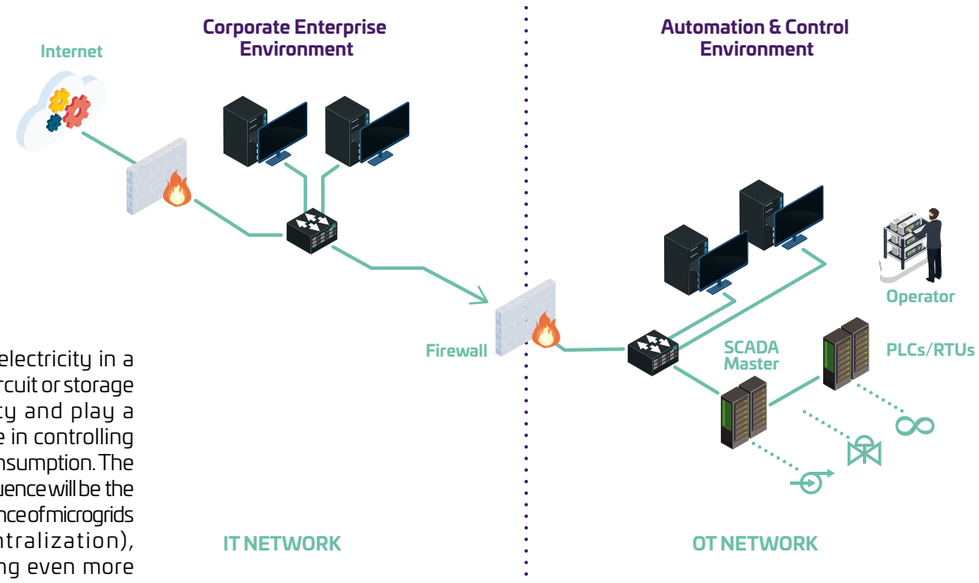
INDUSTRY DYNAMICS

Fossil Fuels
Remains 60%+ of industry and a must to stabilize the grids

Renewables
Fastest growing segment although still less than 50%

Emerging Markets
85% of electricity growth, each country with unique needs

3 - Infographics: GE Internal



While the sector is in transition, the safety of power assets remains a key criterion going forward. Within their changing environment, operators need to cope with new challenges to preserve and maintain the safety functions to avoid any damages or risks to the plant and its full ecosystem. Operators need to implement cybersecurity while maintaining the safety functions of the operations. This is particularly challenging in highly regulated markets like for nuclear power stations. Cybersecurity solutions are required that secure nuclear assets themselves, as well as address the challenges of regulated nuclear power markets.

IT (Information Technology) and OT (Operation Technology)

To discuss cybersecurity in the power industry, it is crucial to understand the difference between IT and OT. Both technologies are differently operated, maintained and connected and have different vulnerabilities to be addressed.

In high-level terms, today's industrial system infrastructure can be segregated into two domains:

1. Information Technology (IT) – systems required for managing data in the context of business goals
2. Operational Technology (OT) or Industrial Control System (ICS) – systems required for controlling and monitoring the physical process and hardware of industrial automation.

As defined by the IEC 62443 automation standard, an Industrial Control System (ICS) is a collection of personnel, hardware, and software that affects or influences the safe, secure, and reliable operation of an industrial (technological) process and associated physical equipment. Industrial Control Systems include but are not limited to:

- Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), Supervisory Control and Data Acquisition (SCADA), and diagnostic systems.
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operational functionality to continuous, batch, discrete, and other processes.

IT security strategies tend to focus on transmission, manipulation, storage and protection of data, and to follow the objectives of the "C-I-A" model: data Confidentiality, Integrity, and Availability. However, for most OT systems, cybersecurity is not about "data" but about controlling and maintaining the continuity of industrial processes. So, in terms of the C-I-A model, "Availability" is a primary concern of security strategies as applied to OT. This is what distinguishes industrial cybersecurity needs from those of other systems, meaning that even most effective classical IT cybersecurity solutions are inappropriate for OT systems, putting the availability (and in some cases the integrity and functional safety) of processes at risk[4].

4 - Infographics: GE Internal

2.1.

Growing Cybersecurity regulations driving demand

Electricity generation, transmission and distribution are all critical infrastructure sectors in the power industry. These sector assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health and safety. The protection of these critical infrastructures at the state and government level is continuously growing in order to cope with new threats.

In the 2000s, the European Program for Critical Infrastructure Protection (EPCIP) or the US National Infrastructure Protection Plan (NIPP) were established.

With several cybersecurity incidents taking place (for example Stuxnet in 2010), cybersecurity attacks were identified as a new major threat to these critical infrastructures. In Europe, the result was the disclosure of a directive on the security of network and information systems known as the NIS Directive (July 2016) which defined obligations to member states to implement national security authorities- and associated laws and regulations- to protect critical infrastructures. Similarly, in the US, several packages of cybersecurity legislative reforms were proposed to increase the level of security of critical infrastructures.

The most common standards and norms describing overall governance, as well as how to implement effective cybersecurity programs, are described in the US NIST cybersecurity framework and the ISO 2700x Series. The specific set of requirements designed to secure cybersecurity in Industrial Control Systems (ICS) and Operating Technology (OT) are most commonly described in the US standard NERC-CIP, the international norm IEC 62443 and the Nuclear standard IAEA – NSS17.

All the above requirements, norms and standards are shaping the power industry globally to specify their cybersecurity needs along with the full product lifecyle for hardware, networks, personnel and training, security management or disaster recovery planning. These requirements are often translated into national law, like the Energy Policy Act (USA), BSI Act (Germany), ANCS (Poland) or LPM (France).

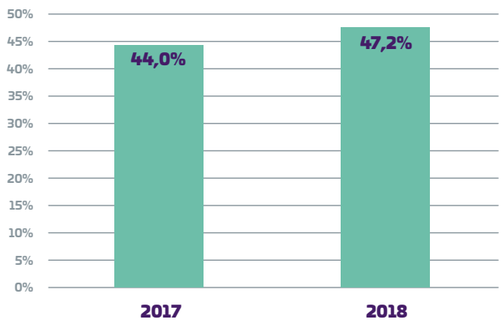
For all critical infrastructures, compliance with these regulations is becoming one of the main drivers for power plant operators to invest in cybersecurity solutions and services.

Cyber threats in Industrial Control Systems (ICS) are increasing

Malicious attacks on ICS and supervisory control and data acquisition systems (SCADA) have increased significantly in recent years. IBM estimated that attacks on ICS increased by 600% between 2012 and 2014. According to Dell in its annual report of 2015, attacks on SCADA-type systems increased more than 7 times over the same period.

According to Kaspersky, on nearly every other ICS device, malicious objects were detected. Industrial PCs are regularly attacked by the same generic malware that afflicts business systems (IT), including (but not limited to) trojans, viruses and worms. In 2018, Kaspersky ICS products across the globe blocked attempted malware attacks on 47.2% of all Kaspersky-protected computers classified as components of industrial infrastructure[5].

Percentage of ICS computers on which malicious objects were detected, 2018 vs 2017



5 - Threat Landscape for Industrial Automation Systems for H1 2018, Kaspersky ICS CERT

The main sources of these attacks are the Internet (25%), followed by removable devices (8%) and Email (5%).

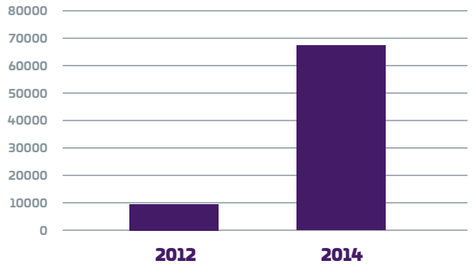
The majority (90%) of today's ICS attacks are commodity type attacks using known vulnerabilities that can be mitigated with common defense-in-depth strategy.

According to the CIS (Center of Internet Security) the majority of attacks on both can be mitigated with basic cyber defense strategies:

1. Inventory and control of assets (Hardware and Software)
2. Continuous vulnerability management
3. Controlled use of administrative privileges
4. Secure configuration for hardware and software on mobile devices, laptops, workstations and servers
5. Maintenance, monitoring and analysis of audit logs

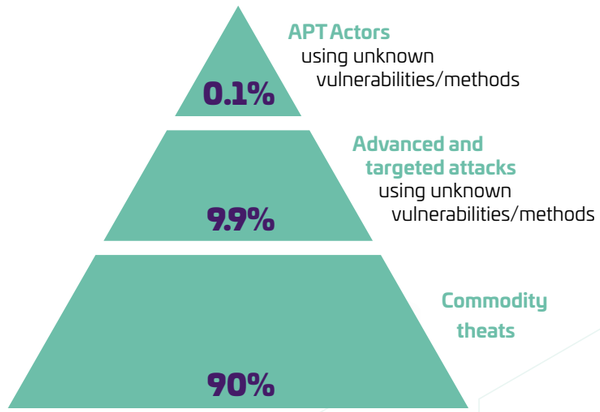
While we see the above being widely spread around IT systems, ICS systems could miss these basic securities.

Growing number of attacks on SCADA systems[6]



According to IBM analyses, attacks on industrial automatic control systems increased by 600% between 2012 and 2014 and according to Dell, in its annual report of 2015, attacks on SCADA-type systems increased by more than 7 times over the same period.

Distribution of the threat according to its nature[7]



6 - https://www.railjournal.com/in_depth/cybersecurity-guarding-rail-against-evolving-threats

7 - Threat Landscape for Industrial Automation Systems for H1 2018, Kaspersky ICS CERT

2.2. Threats facing the sector

Targeted and non-targeted attacks

In order to describe the threat landscape, we need to distinguish between two major types of attacks.

Non-Targeted attacks: Not power sector specific; could be targeting and overall vulnerability in an IT and / or OT system. The main intention is to maximize, spread the attack surface to multiple targets. Often IT focused, via Internet / Email, but also seen on OT / ICS equipment.

Targeted attacks: Specialized on the target or the industry. Often tailored to infiltrate a specific type of equipment and using tailored attack methods. Actors are often extensively planning the attack in detail, having access to above average resources and using unknown methods.

- Requires high technical capacities
- Preferred methodology of APTs (Advanced Persistent Threat) groups
- High risk that specific or unknown ICS vulnerabilities are targeted. Difficult to defend or find
- Impacts on the plant operation or company can be massive

Direct OT attacks often aims to be system disruptive, or destructive. Also, system espionage is a preferred goal.

Indirect OT attacks via IT attacks can take various forms and widely different purposes from espionage, potential reputation damages, disruption until using ICS computing power, e.g to be exploited for crypto mining.

Threat Landscape for Industrial Automation Systems for H1 2018, Kaspersky ICS CERThese different dimensions of the threat[8]:

	TARGETED	UNTARGETED
DIRECT	ATK91 (Xenotime) attack on saudi petrochimical plant	DragonFly 2.0 changes target and focuses on the energy sector
INDIRECT	ATK6 (Havex Energetic Bear) tragets suppliers in the energy sector who offer devices and services for ICS systems	ATK88 (FIN6) crashes Norsk Hydro's OT system with LockerGoga ransomware.

Archetypes of the sector threat and use cases developed

Main attack types on ICS

The major threats on ICS systems today are:

- Social engineering and phishing
- Infiltration of malware via removable media and external hardware
- Malware infection via Internet and intranet
- Intrusion via remote access
- Human error and sabotage
- Control components connected to the Internet
- Technical malfunctions and force majeure
- Compromising of extranet and Cloud components
- (D)DoS Attacks – Distributed denial of service attack
- Compromising of smartphones in the production environment

Among the top 10 threads, the human factor has a substantial impact; especially in environments with ICS equipment. This requires a cultural shift to prevent social engineering, phishing, infiltration of malware via removable media or the human error and sabotage[9].

Internally, changes in sectoral systems, which result in an ever-increasing integration of the IT and OT dimensions create vulnerabilities that attackers can exploit, which can further motivate attacks. Another element is the dependence of users and employees on the proper functioning of these systems, made critical by definition, which invests the consequences of the slightest major attack of a crucial nature for organizations in the sector. This undoubtedly explains the desire to put system security before (missing word here?) security, another opportunity for such attacks. It is not surprising in this respect that the energy sector is one of the most targeted and increasingly focused on its ICS systems.

In Ukraine, the Russian group ATK14 (Black Energy) had deprived between 800,000 and 1.4 million people of electricity and heating for several hours during the winter of 2015[10]. As a result, Industroyer disconnected the Pivnicha high-voltage power plant a year later[11].

These attacks are now tending to increase. In October 2019, India's largest nuclear power plant, Kudankulam (total capacity of 2,000 MWe), was affected by the North Korean group ATK3 (APT38)[12] . The site's IT system was affected but it is not known whether the scenario evolved in a similar way to the attack on Norsk Hydro[13].

In the same month, the British National Cyber Security Center (NCSC) announced an increase in the number of attacks detected- 600 in 2018 alone, and come partly from groups sponsored by foreign countries[14].

A few days later, the NCSC was approached after a nuclear power producer was hit by a major attack.

Finally, at the beginning of December, the ATK40 group (APT34, Oilrig), a well-known Iranian group, targeted the energy sector in Saudi Arabia with its ZeroCleare wiper, which according to our information seems similar to the Shamoon malware created by another Iranian group (ATK50). The sole purpose of these malware are to destroy data even if this would lead to dangerous malfunctions for the infrastructures and staff concerned[15].

Attacks on the sector also target the core of critical infrastructure systems directly or indirectly. This evolution of the threat is not due to chance; we now need to understand the profile of attacks targeting the sector and the functioning of these organizations' systems to find levers for understanding.

8 - The information concerning the attackers and their modus operandi is partly taken from Thales's internal information.

9 - BSI Industrial Control System Security, Top 10 Threats 2016.

10 - https://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/

11 - https://www.welivesecurity.com/fr/2017/06/15/industroyer-plus-grande-menace/

12 - https://economictimes.indiatimes.com/news/politics-and-nation/kudankulam-nuclear-power-plant-in-tamil-nadu-safe-claims-npcil/articleshow/71856380.cms

13 - https://www.cybersecurity-insiders.com/fact-sheet-of-lockergoga-ransomware-which-hit-norsk-hydro/

14 -https://www.ncsc.gov.uk/news/ncsc-defends-nation-against-more-than-600-cyber-attacks

15 - https://duo.com/decipher/new-zerocleare-wiper-malware-used-in-targeted-attacks

2.2.

Threat actors[16]

As well as the diverse types of attacks, different threat actors are active. It´s important to separate their different motivations, resources and technical capabilities to isolate the risks and discuss appropriate measures. It must be noted that there is a fine line between these actors, and a mix of the below must be assumed since there is not always a clear split between motivation / intentions.

A major factor (for targeted attacks) is the threat of APTs (Advanced Persistent Threat) groups. APTs have the characteristic of adversaries sponsored by nation states and at the same level, by cybercriminals and must be considered as continuously high threat, despite the maturity of the sector in terms of security measures. The skill sets and resources (often state sponsored) allow ATPs to threaten any sector, system or organization at any level of cybersecurity and cyber defense. Their motivations are often focused on espionage, but also on sabotage.

Hacktivists will pursue ideological motivations (community, religious, political, etc.) by denouncing facts deemed unacceptable by DDoS attacks, by proselytizing or disinformation through defacement.

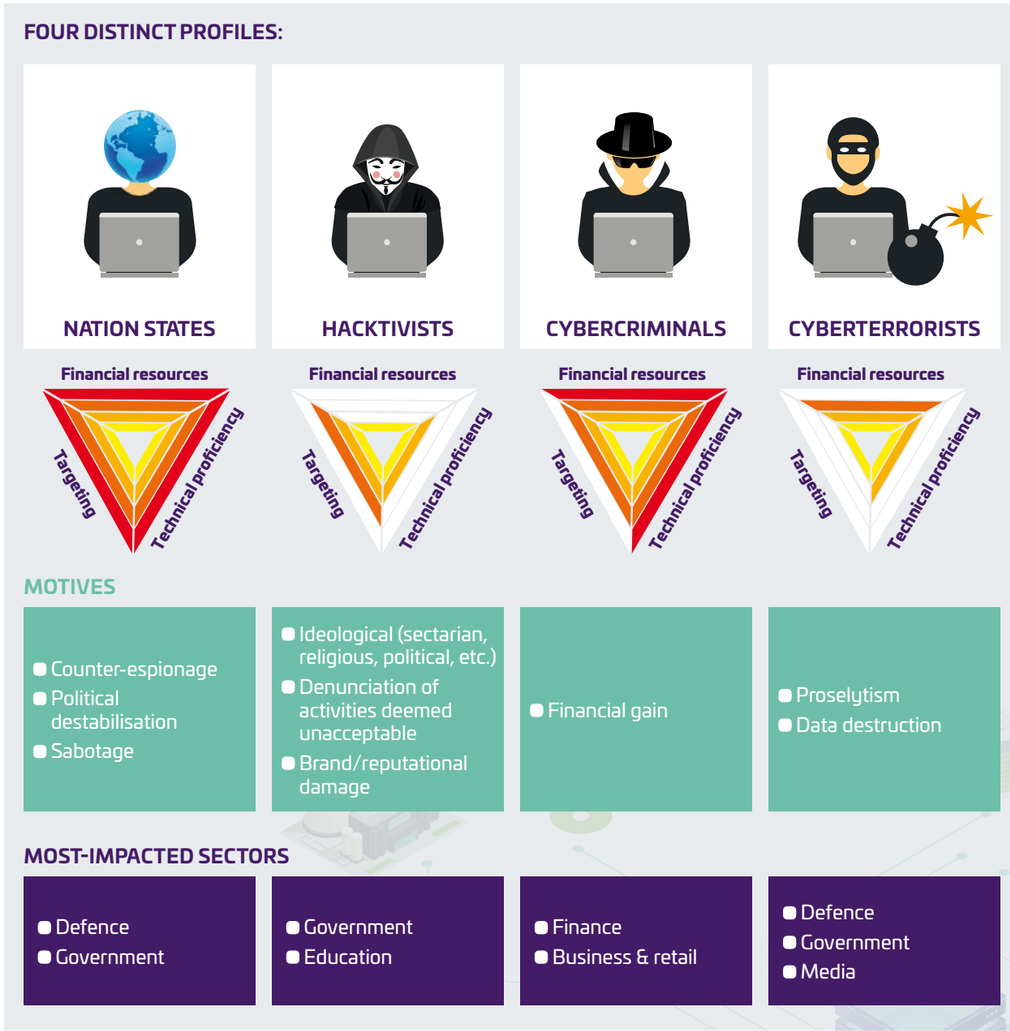
Cybercriminals often have lower skills and motivations that do not have lethal consequences for an organization, literally or figuratively.

Nevertheless, the capacity for nuisance is extremely high and the business, financial, organizational and reputational consequences can be substantial.

Finally, cyber-terrorists, despite media coverage, don't represent a sizable threat in comparison to the first three. (national states, hactivist, cybercriminals) The historical occurrence of cyber-terrorist attacks on the sector is low and cyber-terrorists have historically fewer resources and skills than APTs and major cybercriminals. If we size our protection against the most active cybercriminals today, the protection should be sufficient to cover cyber-terrorists too. Nevertheless, cyber-terrorists have to be observed carefully as one of the main objectives is to weaponize the target for their purposes that could lead to an enormous damage to company and society.

These diverse threats increasingly tend to take advantage of the gateway provided by the IT/OT interface, which is often the soft belly of corporate security because it is poorly understood and unbalanced in terms of cybersecurity levels.

Attackers typology[17]



16 - https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who

17 - Infographics: Thales Internal

3.
THE DIFFERENCE BETWEEN IT AND OT

3.1. Historical Background / Evolution of Environments

Shifting focus of attacks from IT to OT and Increasing Threats[18]

The first software program to be classified as a "computer virus" was written by Bob Thomas at BBN in 1971 and was dubbed "The Creeper." This self-replicating software or "worm" used the ARPANET to propagate between DEC PDP-10 mainframe computers.

Since 1971, the use of malicious software has exponentially increased. While in early phases cybercrime was predominantly known for the theft of data, it rapidly shifted in the 2010s to monetary gain with well known attacks like WannaCry[19]. Beyond the tremendous size of the attack, the ransomware cryptoworm also infected all types of windows workstations without differentiating between personal computers and industrial computers, causing significant damage to various industry sectors. In addition to monetary gain, there are also other motivations that influence the threat landscape to make critical infrastructure systems attractive targets for state-sponsored terrorist groups, or as part of military objectives. Facilities such as electric utilities and chemical refineries or factories are now being targeted to create disruptive influences as political leverage by simply disabling operations or acquiring physical control of resources. A prime example that illustrates the physical consequences of a cybersecurity breach involves the hacking of a dam control system in New York in 2016. The system was offline for repairs when the incident occurred. If the system had been online, the hackers could have operated the floodgate remotely and potentially caused severe flooding during a period of intense rain[20].

Computers and networks are subjected to attacks by hackers at a "near constant rate" of one attack every 39 seconds. Companies with over 5,000 employees experienced a significant crisis annually. Unfortunately, this is the new normal: digital organizations with the complex risk of today render no one to be immune from an attack. According to Cybersecurity Ventures, it is estimated that global cybercrime will cost $6 trillion annually. However, the damage goes far beyond the immediate financial impact. Cyberbreaches cause damage to enterprise infrastructure, both in the online and physical worlds, and also affect third parties such as suppliers and customers[21].

18 - https://pandorafms.com/blog/creeper-and-reaper/

19 - Despite the scale of the campaign, the Wannacry ransomware brought very little income to the group.

20 - https://www.securitymagazine.com/articles/91035-enterprise-wide-risk-management-bridging-physical-and-cyber-protection?oly_enc_id=8564E7018834A6R -- Enterprise-Wide Risk Management: Bridging Physical and Cyber Protection.

21 - October 3, 2019 -- Tim Willis, Security Magazine: Solutions for Enabling and Assuring Business

Contrasting Priorities & Focus

In the IT environment, the hierarchy of concerns associated with data starts with confidentiality followed by integrity and lastly availability, meaning that data is highly controlled and not available for widespread read access. This is contrasted by a complete reversal of concerns in the OT environment where availability of data throughout the entire control network is of paramount importance, closely followed by integrity and of the lowest concern is the confidentiality of the data. Another primary difference between IT & OT environments is that OT systems are inherently designed as isolated environments, and have been for many years prior to the advent of the need to leverage advanced analytics on collected data as well as other related developments. This fact alone is responsible for a relatively large attack surface for the IT environment due to its forward-facing exposure to the Internet, compared to the relatively limited and controlled connection of the OT network to typically only the corporate or IT network and no direct connection to the Internet. In addition, the IT environment is typically comprised of hundreds or thousands of users and endpoint devices whereas the OT environment is typically comprised of only a handful of users and dozens of network-connected endpoint devices.

The modern OT local area network is characterized by separation from the broader wide area network by a firewall device and communication rules and policies as well as administrative constraints that lead to a lower incidence rate of intrusion attempts.

Significant changes have occurred in communication protocols over the years as philosophies have evolved and matured. Initially, ease of use and reliability were prime considerations and security was less important with enabling communication mechanisms. But as exploits proliferated, focus shifted, and more secure protocols evolved such as SSH which has practically replaced the Telnet protocol and HTTPS which has replaced HTTP as more secure. These are only two examples that illustrate the shift from antiquated protocols that pass data as plain text instead of encrypting the transmitted data, which is standard practice with modern protocols where security is a primary requirement in communication networks. The problem with older protocols such as Telnet, FTP, HTTP, and SMTP used in OT environments is

Main technical differences between IT and OT dimensions

	IT	OT
Hardware	Highly integrate network, external firewall	Highly segmented network, multiple DMZ's
Software	Large variety, very dynamic	Limited software applications, very static
Update Cycles	Very frequent (weeks to months)	Sparse updates (quarters to years)
Audits	Format audit procedures, diverse reporting	Random audits but can involve heavy fines
Patches	Weekly to monthly	Quarterly to never
Staffing & Expertise	Large, highly trained staff, big budget	Very limited staff on site
Priorities	Confidentiality, integrity, availability (privacy & avoidance data loss/corruption)	Confidentiality, integrity, availability (System & operational integrity - Maintain operations)

3.1.

Contrasting Priorities & Focus

the lack of "strong" encryption that makes them fundamentally susceptible to hackers using sniffing technology on the network. To deploy an effective "defense-in-depth" strategy, all protocols regarded as weakly encrypted should be disabled by default, and methods such as "Group Policy Objects" must be configured to enforce configuration adherence to the use of only the newest, strongly encrypted protocols.

It should also be noted that the configuration of the OT environment is relatively static compared to the very dynamic IT environment where users are typically installing and uninstalling new software, creating, modifying, and deleting files, upgrading software, etc. There are typically automated processes which apply software patches on a regular basis and are constantly manipulating user data as well as policies, whereas in the OT environment, users are typically logged in for an entire shift and will typically run less than a handful of executable programs. There is a constant set of system services running on each endpoint and these executables are seldom modified, and even security patch updates occur with no greater frequency than monthly and often no more than quarterly or annually. Patches are required to be validated and approved by the OEM before being applied to ensure that no malfunction of the control system will occur and prevent injury to personnel or damage to equipment. Additionally, the OT operational schedule is typically 24x7, offering a lack of frequent or regular maintenance windows to apply updates which may not even be available. These concerns do not exist in the desktop environment of the IT world.

3.2. Cyber and Safety in OT environments

(Design for functional safety)

One of the main challenges for critical system infrastructures are the system safety levels. These must be maintained at any time, as well as when cybersecurity measures are deployed to improve security.

Especially for cybersecurity in nuclear applications, specific challenges must be addressed by the specialized domain experts.

While the common IT cybersecurity concepts are built to follow threats evolution and to update regularly the system to be at the right level of protection against new vulnerability disclosed, OT safety concepts are designed to limit modifications. OT safety system evolutions often require an impact analysis and a design change approval from the customer for each system change (sometimes even from safety regulators, e.g. in the case of Nuclear Plants). In some cases, when implementing significant system modifications (e.g. cybersecurity by design), it could even impact the safety certification level and associated qualifications.

Design cybersecurity for functional safety

It requires domain expertise to balance the right level of cybersecurity with acceptable impact on the existing system. Before implementing cyber solutions into an existing OT environment, the system architecture, all network elements, their related functions and the interactions related to functional safety have to be fully understood. By analysing the various vulnerability and threats, the risks and impacts in relation to the safety functions have to be carefully addressed. Depending on the criticality of the component and associated process function, security measures must be adapted. Decisions have to be made, e.g. to fix, contain or isolate vulnerabilities. The defense-in-depth strategy with several passive and non-intrusive measures as well as strong and cumulative protection at the periphery of the safety system must be adjusted and deployed to ensure full safety and compliance.

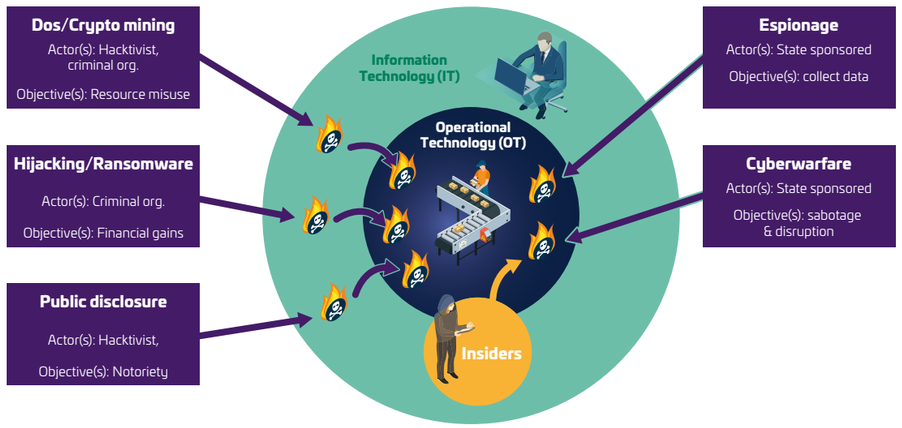
3.3. Specific OT vulnerabilities/ challenges

The relatively small userbase of the OT local area control network and lack of a direct connection to the Internet or email greatly diminishes the attack surface available to ambitious cybercriminals compared to the much more exposed IT environment. This difference tends to influence hackers to utilize the IT network as an easier attack vector into OT (indirect attack). Forensic analysis of some focused attacks on critical infrastructures show that access to the control network was gained by first compromising the more exposed IT network. The preferred attack vector is often a successful email phishing campaign that either sophisticated malware to be installed which later allows successful harvesting of usernames and passwords and network architecture.

The dynamic and large installed software collections in IT environments require exceptional vigilance by a large staff of security experts. Maintaining compliance with security patch updates and awareness of the latest vulnerabilities requires the effort of a full-time staff dedicated to these functions alone. Users are constantly acquiring new software applications or upgrading their existing software libraries. In the OT environment, change is tightly controlled and very limited. Change leads to risk which cannot be tolerated in a 24x7 operational environment where revenue is generated by close to 100% uptime and efficiency. This static software baseline is much easier to characterize and monitor for anomalies, and also lends itself to a specialized set of software tools for protection.

An additional challenge of the OT environment is the patching process. While the IT environment accesses the corporate WAN, it allows for automated patch updates from secure sources monitored by staffed operations centers. These avenues do not exist in the classical OT environment. OT patching needs a specific attention to eliminate newly discovered vulnerabilities, for example a more manual management and deployment of security patch updates.

Examples of Direct vs In-direct OT attacks and objectives[22]



22 - Infographics: GE Internal

3.4. OT vs. IT Cybersecurity Products

The differences between IT and OT environments give rise to somewhat divergent approaches to the security measures that are implemented to protect them from attackers. Both environments benefit greatly from the employment of an Active Directory domain implementation. A healthy security patch management program is also paramount to securing both environments. However, the difficulty of applying patch updates in a timely fashion for the OT domain demands additional "defense in depth" strategy. Fortunately, the very static software environment and limited library of executable code facilitate the use of various methods of "white listing" which will control permission to run on each platform in the OT control network. All executables can effectively be cataloged and characterized. Any changes to the executable files or new files can be easily identified by specialized software applications and blocked from execution. This is one of the most effective methods of protecting control systems in the OT environment from being compromised by malware. The white listing approach is more effective than installing traditional anti-virus software applications that are useless against newly discovered zero-day threats for which virus definitions have not yet been updated in the application.

4.

USE-CASES OF OT ATTACKS AND TECHNICAL DEEP DIVE

4. Use-Cases of OT Attacks and Technical Deep Dive

The best way to assess the threat is to consider the characteristic use-cases. These various cases do not in any way claim to be exhaustive, as the threat landscape is vast and complex. Nevertheless, they allow us to consider the forms of attacks imaginable on an OT system (of the ICS type):

1. First, the case of ATK91 (Xenotime) to illustrate a targeted and direct attack

2. Then the case of DragonFly 2.0 for a non-targeted and direct attack

3. In the third case, the LockerGoga ransomware to consider the case of an untargeted and indirect attack

4. Finally, a very elaborate attack passing through the supply chain of the sector in order to study the case of an indirect targeted attack

4.1. ATK91 (Xenotime): the new decisive threat to the energy sector[23,24,25]

Group description

Aliases
- ATK91
- XENOTIME
- TEMP.VELES
- TRITON GROUP

Motivation

Attacks on industrial security systems almost exclusively with destructive intent

Trageted country

Spatialization of the Xenotime attack

TRITON is a very sophisticated malware allowing the manipulation of Industrial Control Systems (ICS) of critical infrastructures discovered at the end of 2017 when it caused an accidental shutdown of the machines of a petrochemical plant in Saudi Arabia. The attacker's tools and TTPs indicate that he has prepared to conduct operations that can last several years. . In the 2017 attack, the group compromised the target's network almost a year before reaching the Safety Instrument System (SIS). During this period, priority seems to have been given to operational security. His lack of "curiosity" during the operation may indicate that the aggressor was still in the preparation phase and that his real targets had not yet been determined.

It is difficult to definitively determine the motivation behind this campaign. According to several observers, the main objective of the latter was to test the tools and refine the techniques. It should be noted that according to Dragos, the Triton group (Xenotime) is probably one of the most dangerous groups known to date, since it attacks industrial security systems almost exclusively with destructive intent causing loss of life.

23- TRISIS Malware Analysis of Safety System Targeted Malware, Dragos.
24 - Thales internal information.
25 - https://www.industrie-techno.com/article/le-recit-par-schneider-electric-de-triton-l-attaque-qui-a-fait-trembler-l-industrie.57306

4.1. ATK91

This use case demonstrates that while direct destructive attacks by groups sponsored by third states on such infrastructures are relatively rare, they are not inexistent. Alder the geopolitical tensions that we know, the organizations of the sector must keep in mind that they can be the privileged targets of groups motivated geopolitically by higher interests.

Course of the attack

At the end of 2017, an oil and gas installation in Saudi Arabia was shut down due to infection by a strain of malware capable of interfacing with the installation's industrial control systems. This malware was aimed at Schneider's Triconex instrumented security system. Access to the system was carried out in the traditional way with phishing and identity hacking by changing the telephone number to receive the SMS, giving the administrator password. The group then compromised a system administrator workstation, after having laterally crossed the demilitarized zone constituting the airlock between the IT network and OT. The identifiers were then used to access the SIS controllers to compromise them. The controllers were placed in "Program Mode" during their operation, allowing the attackers to reprogram them. The attackers stayed for nearly a year in the system's engineering station. It is from this starting point that they were able to send a trojan horse to infect the memory of SIS automatons via the operation of a zero-day, allowing an increase in privilege. Since then, the attacker has had full control of the plant. One year after the intrusion, on June 3, 2017, Xenotime went into attack mode. Soon, the procedure for securing the petrochemical plant was triggered and the temperature and pressure began to drop. The machines stopped in an emergency. Two months later, almost to the day, the same phenomenon occurred and suggested a major cyber-attack.

It is believed that during the first attempt the group inadvertently closed the installation, as some controllers stopped themselves when their logical code failed a validation check. The protocol attacked by the group is proprietary, which suggests prior reverse engineering. In addition, the development of the tool would require access to both hardware and software that are difficult to acquire. Such an attack requires deep technical knowledge and, although probably not reproducible on a large scale, it shows that the attacker is sufficiently capable to attack and potentially cause physical damage to plants and industrial systems. The group would be linked to the Central Institute for Scientific Research in Chemistry and Mechanics in Moscow for the following reasons:

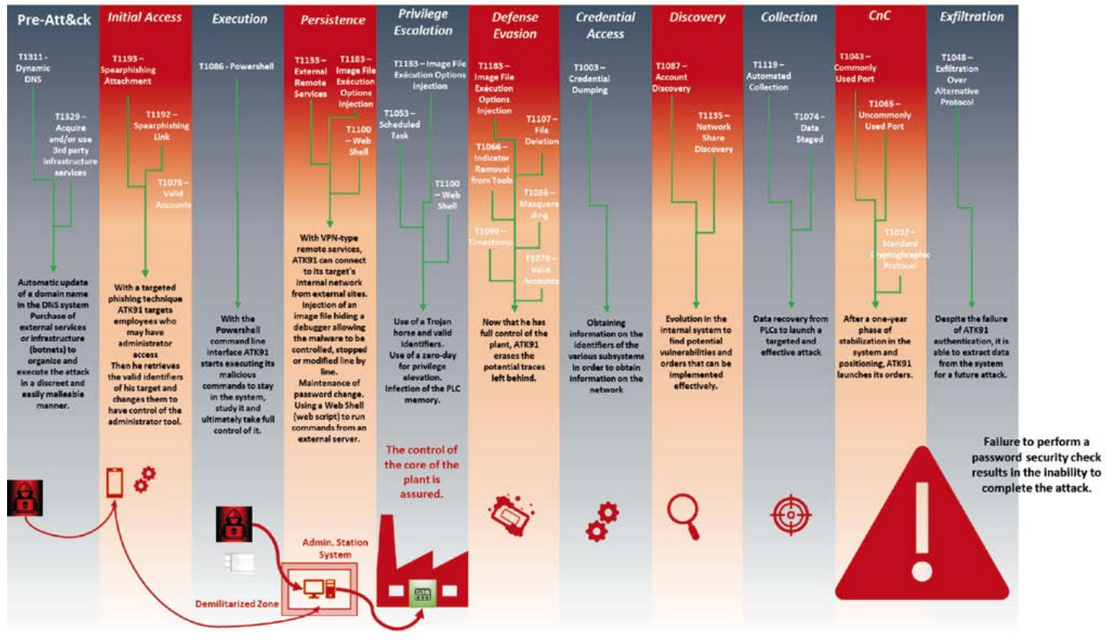
- Personal links with this Institute
- An IP address used by the attacker
- Correspondence between working hours and working hours in Moscow

The group has been using test environments to test the internal workings of its malware since at least 2013. Further intrusions were carried out by this attacker in the Middle East on undisclosed dates, focusing on oil and gas companies until the end of 2018. It should be noted that the group has also begun to survey energy systems in the United States and other countries.

Xenotime uses a dozen personalized and public tools to carry out its attacks. Custom tools reimplement the functionality of public tools by adding anti-detection methods. These tools seem to be used during the critical phases of the intrusion.

Attacks on industrial systems are long (several months or years) since they require learning how to exploit the target's industrial process and developing the appropriate tools. The attack is therefore preceded by a discovery, learning and preparation phase during which the attacker will set up his attack infrastructure. The infrastructure uses VPS servers from international hosting providers (OVH or UK-2 Limited), VPN and Dynamic DNS to change IP addresses regularly. After entering the target's network, the attacker needs to ensure persistent and very discreet access throughout the mission.

Tactics, Technics et Procedures used by Xenotime



Xenotime therefore uses several methods to hide its activities:

- Rename the files to look legitimate (using the Microsoft Update file nomenclature)
- Use of standard tools simulating an administrator's activity (RDP, PsExec, WinRM)
- Editing legitimate Outlook Exchange files to open web access
- Use of encrypted communication for sending commands and programs
- Use of multiple sub-folders rarely used by users or programs
- Regular cleaning of attack tools, activity logs, temporary files after use
- Changes to the dates contained in the files (creation and modification date)
- Use of VPN networks, allowing to hide the attacker's IP address

The persistence of malware on compromised machines is achieved by creating an "Image File Execution Options" registry key or scheduled tasks. After reaching the targeted SIS controllers, the attacker focuses on deploying TRITON by limiting his activities to off-peak hours to avoid being discovered. TRITON then allows full control of these systems.

This modus operandi, which is largely based on the concern for non-detection, allows us to draw two conclusions. First, this development axis is typical of state-sponsored attackers. The latter not wanting to be linked to offensive computer fight logic with a geostrategic dimension requires groups to fund them with the greatest discretion. In this case, the fact that the group is linked to a national research institution and that its modus operandi is devoted to destruction reinforces this hypothesis. The second conclusion that can be drawn from this emphasis on concealment is that it confirms the non-operational nature of the attacker's arsenal at the time of the attack. The ambition is to stay as long as possible in the target's systems to test his tool more and more. The case of this group shows that the theory of security by darkness, consisting in thinking that an ICS/SCADA system is complex and therefore secure, no longer holds. The rise of attacker groups, the generalization of protocols and the standardization of systems have changed the situation.

3.2. DragonFly 2.0[26,27,28]

Group description

DragonFly is an espionage group, that has been active since at least 2011.

The group led a campaign in 2015 named "DragonFly 2.0" by Symantec. This campaign is focused on the energy sector, and has mostly two different goals:

- First, gaining information about the operational aspect of the energy sector, notably by stealing documentation
- Second, getting "first-hand" experience of the way these systems work, by gaining access to these facilities

Symantec asserts that the group has gathered enough knowledge and information to cause destructive action and sabotages should the group decide to change its objectives.

The campaign started in 2015 and has targeted organizations around the world, including the United States and Turkey (two recurrent targets of the group) and Switzerland.

The group uses multiple techniques in order to get to its victims, but none of them are specific to industrial control systems. Indeed, these attacks are focused on IT systems and most of the time work by abusing the user's naivety. Among the common techniques used by the group, we can find spear phishing emails, a technique that the group used with increased intensity between 2016 and 2017, watering hole attacks, as well as programs containing trojans.

The group uses the Phishery tool in order to send their emails, a tool that became available publicly on GitHub.

These techniques allowed the group to harvest credentials of users in the sectors that it considered relevant.

The group was able to move onto the next step, and use this information to insert backdoors (in this case a malware named Goodor) in servers.

> This use case demonstrates that we should not consider that the best attackers are by definition specialized in targeting a particular sector.
>
> Cyber threat surveillance must be global since an unknown attacker on a sector can suddenly become formidable even when it comes to attacking complex security systems like ICS.

26 - https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
27 - Thales internal information.
28 -https://fortune.com/2017/09/06/hack-energy-grid-symantec/

A group seeking operational information

While the original campaign of the group was focused on gathering technical information, this new campaign seemed to be more specifically focused on operational information: For example, the group took a large number of screenshots, and especially of machines that had access to control systems.

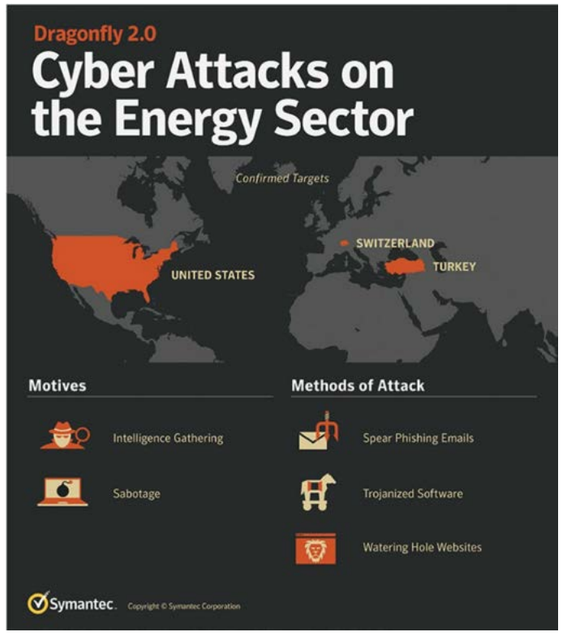
Interestingly, the group likes using off-the-shelf malware, potentially in an attempt to make attribution harder. This assumption is reinforced by the presence of strings in different languages, indicating that at least one of these languages act as a false flag.

The group does not use zero-day vulnerabilities, potentially because of a lack of resources.

Another group, named DragonFly was already known, but security researchers are not all agreeing on whether the DragonFly 2.0 is actually the work of this group: Symantec strongly suggests so, notably because of a shared malware. However, CrowdStrike believes that the link is not strong enough to link them. They note that the common malware leaked in 2010, allowing any other attacker to impersonate the first group[29].

Symantec has seen the attacker targeting more than 100 corporations and have notified them.

The fact that the group did build a list of credentials might mean that removing the malware on the infected systems may not be enough. Changing the passwords must be done on every person that might have been the victim of the group.



Summary of recent DragonFly 2.0 attacks

29 - https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

4.3. ATK88 (LockerGoga) attacks on NorskHydro[30,31]

Early stages

LockerGoga was first identified on January 22nd on a malicious website collecting instructions to remove malware from its system. Two days later, extracts of the code, one from Romania, the other from the Netherlands, were uploaded to the VirusTotal platform for analysis. It should be noted that Altran has subsidiaries in these two regions and was affected less than a week later.

Attack on Norwegian industrialist Norsk Hydro via ATK88 (LockerGoga) ransomware

On March 19, Norsk Hydro announced that it had switched to manual mode or temporarily stopped aluminum production in several plants following a cyber-attack. The Norwegian National Security Authority (Nasjonal Sikkerhetsmyndighet) and local media describe the incident as a ransom attack by LockerGoga malware. The attack apparently paralyzed the company's computer systems. Norsk Hydro is one of the world's largest aluminum producers. Some of its facilities were affected by the attack, causing failures or a switch to manual control systems. The attack had an impact on aluminum production.

According to media reports, the attack began on the evening of Monday, March 18, Oslo time (UTC + 1). On March 19, the company's website was not available and production impacts were reported:

- The tank lines, which monitor the molten aluminum and must operate 24 hours a day, have been switched to manual mode;
- Some plants have been forced to stop production;
- Several metal extrusions plants have been closed;
- In some installations, computer systems are not available and printed orders are executed;
- The power plants are operating normally;
- No security incidents were reported.

30 - Thales internal information.

31 - https://www.cybersecurity-insiders.com/fact-sheet-of-lockergoga-ransomware-which-hit-norsk-hydro/

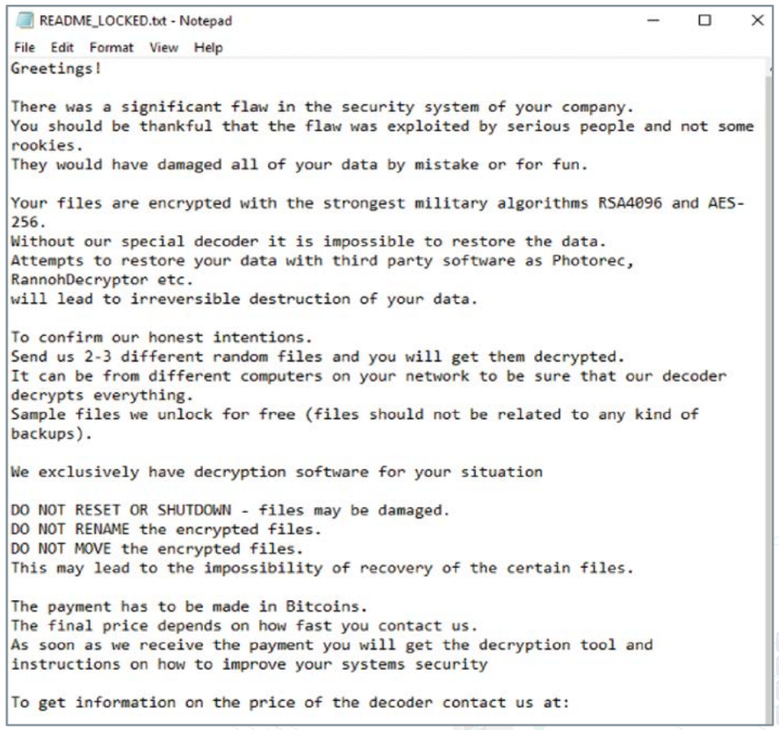
Description of the ATK88 (LockerGoga) scenario in the case of Norsk Hydro

If after a preliminary analysis of a LockerGoga sample with the SHA256: 6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77

The malware encrypts files with one of the extensions listed below as a priority, then encrypts the other files: (do[ct][xb]?|wbk|xlm|xlsx|xltx|xlsb|xlw|pp[ts]|pot|p[op][st]x|sldx|pdf|db|sql)

The extension types indicate that the main objective of the threat actor is to encrypt files containing data important to users. At the end of the encryption sentence a file called "README_LOCKED.txt" is placed on the desktop containing the following message:

Message displayed on the computers of LockerGoga victims at Norsk Hydro



4.3. LockerGoga attacks on NorskHydro

How ATK88 (LockerGoga) works

The malware encrypts all files, and in priority those with specific extensions. He then places the ransom request in the file system. Users are then informed of the necessary steps to recover the files. Malware does not have the ability to spread to other targets. Nevertheless, it seems to use anti-analysis techniques to avoid detection. For example, it seems to detect the presence of a virtual machine and has the ability to erase itself from the file system to avoid collecting samples.

Since threat actors have not added any customized or complex features to the malicious code (C&C, DNS tagging, etc.), Nozomi Networks assumes that the expected impact is disruption rather than espionage. However, it is established that the malware destruction capacity has increased.

Malware does not have any special capabilities linking it to the company or industrial control systems. Thus, it is likely that the company was not targeted, and that the infection was done using traditional initial access means (Spam, brute force attack using default identifiers...)

Some researchers have suggested that attackers may have used Active Directory as a mechanism for spreading malware. A possible scenario (confirmed by NorCERT):

- Threat actors may have infected a system registered in the Domain Admin Group of the target organization;
- The malicious executable has been placed in the Netlogon directory so that it can be automatically propagated to each domain controller;
- Many firewalls accept Active Directory information by default

Identify and eliminate ATK88 (LockerGoga)

The infection is identifiable because the targeted files will be encrypted and the". locked" file extension will be added at the end of the file names. The only known way to remove LockerGoga from a system is to restore from a backup.

Norsk Hydro uses innovative means of communication in its incident response. Unlike Altran, Norsk Hydro has adopted a completely different communication approach. They quickly created a live information session on the attack by providing regular updates on their Facebook channel.

Norsk Hydro's response restored the systems quickly and minimized the financial losses of the attack. This reaction has been described as particularly effective and can be considered as a reference.

To minimize the risk of your system being affected by LockerGoga, it is suggested to:

- Communicate with employees on how to recognize a phishing email and what to do if they think they have received one;
- Ensure that systems have up-to-date backups;
- Monitor your systems with solutions that quickly identify malware, compromise indicators and behavioral anomalies.

Through this example we understand that even a ransomware attack on the IT system of a company can have fatal consequences on the OT system of the victim. A good knowledge of IT-OT interfacing is necessary in order to avoid aggravating the consequences of an attack.

4.4. Havex from ATK6 (Energetic Bear)[32]

Group description

In 2014, the EnergeticBear / Croutching Yeti / Dragon fly group targeted companies to develop programs to support ICS. The targets were MESA Imaging, eWON, MB Connect Line GmbH.

The Backdoor Havex is developed and used by the Energetic Bear Group, an APT group sponsored by the Russian government that specifically targets organizations in the energy sector as well as companies in other ICS sectors such as industry/machinery, manufacturing and pharmaceuticals.

An effective supply chain attack strategy

It is interesting to focus on suppliers who have been compromised because, even if we do not really know the second intention behind the backdoor Havex, this event teaches us several things about the supposed weaknesses of these systems in the eyes of the attacker.

Thus, three different suppliers were affected:

- MESA, a Swiss company that manufactures industrial quality cameras for distance measurement, acquired by Heptagon[33],
- eWON, a Belgian company that provides remote maintenance services for industrial control systems: "Talk2M[34]" used in 156 countries around the world that can be spied on,
- MB Connect Line GmbH, a German company that sells mbNET industrial routers and a VPN service: VON mbCONNECT24[35].

We realize that our diagnosis of potentially risky devices and services is not without relevance. Several hypotheses can be made based on the limited information available.

Energetic Bear voluntarily targets suppliers of distance calculation cameras which, if infected by design, can allow advanced spying on a critical industrial infrastructure. Interconnections with security systems can also allow lateral movements in the system.

Then a company that provides remote maintenance services for industrial systems. The Talk2M service is composed of VPN servers based mainly in Europe that allow communication with critical infrastructures in 156 countries. The attacker can therefore observe these infrastructures with legitimate access and corrupt maintenance communications for sabotage, for example.

Finally, the products developed by MB Connect Line GmbH are first of all routers specific to ICS systems and a specific VPN service. The company in question describes its router as follows: "*mbNET industrial routers have been specially designed for industrial use. They provide a reliable and secure connection of machines and installations via the Internet. They support various security protocols and are universal.[36]*"

It is easy to understand that the compromise by design of this type of router could allow orders to be launched from outside to inside the system by erasing the interface security between the IT and OT networks.

For the German company's VPN service: "*mbCONNECT24, MB connect line's remote service portal, is a platform for remote maintenance and data logging, alarm, web visualization and M2M[Machine to Machine] communication.[37]*"

Compromising such a service would allow the attacker to place orders on maintenance services, spy on the system via data logging, compromise alarm systems and place orders from machines to machines.

32 - https://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans
33 - https://ams.com/ams-start
34 - https://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans https://ewon.biz/cloud-services
35 - https://www.mbconnectline.com/en/products/mbconnect24.html
36 - https://www.mbconnectline.com/fr/produits/mbnet.html
37 - https://www.mbconnectline.com/de/produkte/mbconnect24.html

4.4. Havex

An indirect attack against ICS systems

Finally, it is interesting to note that the target companies are exclusively European and that mbCHECK has only been compromised in its version for European users. The attack that followed this first compromise thus targeted European actors as a priority. Other information that can be deduced from this set of attacks is that they are not uncorrelated to each other.

Indeed, compromised devices and services are indeed critical individually, and could allow harmful attacks on any sector of activity. However, if we look at the articulation of compromised devices and services, we understand that a large-scale attack was being prepared.

Let us consider this sequence:

A hypothesis can be made of a first step consisting in taking control of the IT/OT interface through the compromised routers of MB Connect Line GmbH, followed by a compromise of the remote maintenance (eWON) of the system preventing the detection of the compromise of the first compromise.

Once the interface is disarmed, and the maintenance system infected, MESA cameras could be compromised to mislead operators. Operators could not be alarmed in case of malfunction of these same cameras since MB connect line's remote service portal could no longer send alarms or healthy communication with other machines.

Attacks using HAVEX thus draw serious compromises of different devices and services, but taken together they suggest an even greater threat, that of preparing an end-to-end and extremely effective kill chain from the IT system.

The example of Havex from ATK6 (Energetic Bear) is symptomatic of the new practices that we are seeing in the cyber threat landscape.

Attackers arm themselves with patience, study the indirect possibilities to carry out efficient and discreet attacks by dissecting the supply chain of their targets. Sometimes, as in the case of Havex, this fine knowledge of the target supply chain is accompanied by a formidable ability to compromise a system brick from its design phase to make the attack almost unstoppable and undetectable.

Screenshot of the MESA Imaging pilot installer trojanized

Company:	MESA Imaging
Product:	Swiss Ranger version 1.0.14.706 (libMesaSR)
Filename:	SwissrangerSetup1.0.14.706.exe
Exposure:	Six weeks in June and July 2013 (source: Symantec)
Backdoor:	Sysmain RAT
MD5:	e027d4395d9ac9cc980d6a91122d2d83
SHA256:	398a69b8be2ea2b4a6ed23a55459e0469f657e6c7703871f63da63fb04cefe90

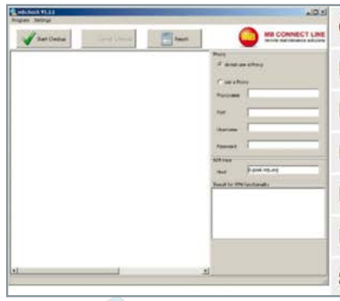
Screenshot of the Talk2M eCatcher installer trojanized

Company:	eWON
Product:	Talk2M eCatcher version 4.0.0.13073
Filename:	eCatcherSetup.exe
Exposure:	Ten days in January 2014, 250 copies downloaded (source: Symantec)
Backdoor:	Havex 038
MD5:	eb0dacdc8b346f44c8c370408bad4306
SHA256:	70103c1078d6eb28b665a89ad0b3d11c1cbca61a05a18f87f6a16c79b501dfa9

Screenshot of the mbCONFTOOL installer trojanized

Company:	MB Connect Line GmbH
Product:	mbCONFTOOL V 1.0.1
Filename:	setup_1.0.1.exe
Exposure:	April 16 to April 23, 2014 (source: MB Connect Line)
Backdoor:	Havex RAT 043
MD5:	0a9ae7fdcd9a9fe0d8c5c106e8940701
SHA256:	c32277fba70c82b237a86e9b542eb11b2b49e4995817b7c2da3ef67f6a971d4a

Screenshot of the mbCHECK app trojanized



Company:	MB Connect Line GmbH
Product:	mbCHECK (EUROPE) V 1.1.1
Filename:	mbCHECK.exe
Exposure:	April 16 to April 23, 2014 (source: MB Connect Line)
Backdoor:	Havex RAT 043
MD5:	1d6b11f85debdda27e873662e721289e
SHA256:	0b74282d9c03affb25bbecf28d5155c582e246f0ce21be27b75504f1779707f5

38 - https://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans

4.5. Potential impact of an attack in the Power Landscape

Independent of the motivation or source of a cyber-attack, the consequences are significantly higher than measures to avoid them. It´s important to highlight that the majority of attacks can be easily avoided with basic cybersecurity strategies.

To illustrate the theoretical impact, we will describe two cyber-attacks on an ICS system of an 800MW power station. In this example we assume power station is not protected.

Three typical consequences must be assumed:

1. Financial impact due to downtime, system recovery, asset aging, and replacements
2. Safety impact due to malfunction of certain equipment
3. Indirect consequences: Broader environmental impacts (Reputation, Blackout, ...)

While the impacts in the above example are theoretical, it's important to stress that financial risks are real. For example, the "NotPetya[39]" attack in 2017 led to damages of:

Pharmaceutical company Merck	**$870 million**
Delivery company FedEx (through European subsidiary TNT Express)	**$400 million**
French construction company Saint-Gobain	**$384 million**
Danish shipping company Maersk	**$300 million**
Snack company Mondelēz (parent company of Nabisco and Cadbury)	**$188 million**
British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)	**$129 million**
Total damages from NotPetya, as estimated by the White House	**$10 Billion**

Theoretical Impact Analysis
(800MW Power Station with limited Cybersecurity)

		Case 1 Non-targeted attack	Case 2 Targeted attack
	Type/Risk level	Commodity threats high (90% of ICS attacks)	Designed attack medium (10% of ICS attacks)
FINANCIAL	System downtime Root cause analysis/ System recovery (loss of revenue)	Multiple days (~$5M+)	Weeks - Months (~$15M+)
	Equipment	Partial recovery PC's/ server/network/HMI (~$0.5+)	Up to full replacement
	External expertise (root cause & recovery)	Mid-level expertise (1000$ per day/head)	High-level expertise (3000$ per day/head)
	Contractual Liabilities (e.g. in case of PPA*)	LD's ($125k-$250k per week)	LD's ($125k-$250k per week)
	TOTAL	$8M+	$20M+
INDIRECT	Reputation/media	Low-medium risk	High risk
	Competition/suppliers	Low-medium risk	High risk
	Blackout	Low-medium risk	High risk
SAFETY	Impact of plant safety systems	Low-medium risk Controlled forced outage	Critical Risk Manipulation/ Misfunction

*PPA: Power Purchase Agreement

39 - https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

5.
CONCLUSION AND RECOMMANDATIONS

5. Conclusion and Recommandations

Thus, the landscape of the cyber threat to the energy sector and its industrial control systems follows the evolution of the cyber threat in the broadest sense. It evolves, becomes more complex and requires permanent and specialized monitoring. Through this report we have determined that the critical ICS/SCADA systems used by organizations in the sector are more and more provoke envy of attacks from state-sponsored groups in particular. Geopolitical, social and economic movements could therefore be sufficient reasons for such attacks on the sector. This dynamic is further reinforced by the trend towards the increasing interconnection of the IT and OT dimensions of organizations. This is an unlikely but highly dangerous threat.

Attacks that are not necessarily successful in themselves but are extremely likely must also be considered. Those include untargeted attacks such as Ransomware but also the extension of the supply chain and the multiplication of vulnerabilities on the devices that are traded in its entirety. Coupled with the structuring of the Malware-as-a-Service phenomenon with the availability of identifiers and botnets creates porosities that allow attackers to envisage new attack campaigns.

By analyzing and understanding these phenomena, it is possible to envisage relevant detection and mitigation solutions. The aim is not to be unnecessarily alarmist but to make the right diagnosis to offer the right solutions in order to avoid the greatest torment.

The operational recommendations are based on the good practices raised by the ANSSI in terms of securing Industrial Control Systems[40]. While it's highly recommended to implement the same recommendations in OT environments than in IT environments, it must be highlighted that these can't be always be executed due to the state of the system (e.g. Patches or Anti-Virus not possible). In such a case it is important to contain the vulnerability on the periphery by implementing a proper defense in depth.

40 - https://www.ssi.gouv.fr/uploads/IMG/pdf/Guide_securite_industrielle_Version_finale-2.pdf/

Recommendation (Strategic): Know your system

Do very detailed Asset Inventory, identify Legacy systems and Safety Functions, formalize associated constraints and process criticity. Use system testing tools such as Cyber range. Perform regular system audit campaigns.

Recommendation (Strategic): Learn about threats/vulnerabilities

Use Cyber Threat Intelligence (CTI) service for prioritizing the threats to be taken into account, according to its internal parameters: system architecture, devices present with their vulnerabilities, etc. Thematic sheets related to the evolution of the threat stakes in order to adapt its protection strategy. Acquire detection capabilities such as Intrusion Detection System (IDS), Honeypot and Deception Technology.

Recommendation (Strategic): Upgrading the supply chain

Develop a constructive dialogue on cybersecurity with suppliers/partners. Perform Audit on critical systems used and/or provided by Suppliers. Clearly define the "Due diligence" of suppliers' liabilities concerning cybersecurity prior to agreement. (including Mergers and Acquisitions (M&A) process).

Recommendation (Strategic): Implement Defense in Depth

Objective is to reduce attack surface when vulnerability can't be fixed by a patch due to industrial, availability and safety context. Sometimes patch is not possible in ICS. Concept is to define and implement number of technical cumulative measures and remediation actions at the periphery of the system, combined with organizational and procedural ones.

Recommendation (Strategic): Have an integrated vision of securing IT/OT/IOT devices and systems

Take into account the special features of IT/OT/IOT systems. Consider the articulation of these systems according to their particularities (difficulty to patch ICS systems for example). Have a bottom-up approach in the vision of security, from the product to the system, to avoid compromise by design.

Recommendation (Operational): Management of removable devices

Define a policy for the use of removable devices. Disallow the use of removable devices and use airlocks to exchange data if necessary. Restrict functionality or disable USB ports on systems.

Recommendation (Operational): Account Access management

Define a policy for managing user and application accounts. Do not leave default accounts on devices and applications. Force the definition & use of strong passwords. Force the periodic change of account passwords.

Recommendation (Operational): Hardening of configurations

Install only the necessary software, protocols and services. Perform audit to check that no development tools are present on production servers or operator stations. Force the use of control avoiding default choices. Systematically disable vulnerable and insecure protocols and features and also disable automatic configuration & discovery protocols. Disable remote configuration and operation mode management on critical installations.

5.

Recommendation (Operational): Event and alarm log management

Enable monitoring & system events generation functions if the equipment and software allow it (such as syslog, SNMP V3, Windows Event, text file, etc.). Limit to the relevant events and organize their storage (volume, storage life). Centralize logs and generate alerts for certain events or event sequences.

Recommendation (Operational): Configuration management

Perform periodic comparison between programs and configurations active in the devices and the backed-up version identified as the reference. Audit new version and analyze/justify the differences with the previous before commissioning the new version.

Recommendation (Operational): Backups/restores

In order to be able to recover rapidly the system in case of attack, define a backup policy including what data needs to be backed up to meet user needs, rebuild an installation or meet regulatory requirements. Perform periodic verification of the backed-up data by restoring part of them.

Recommendation (Operational): Documentation

Define a documentation management policy (update process, retention period, mailing list, storage...). Securely store the documentation relating to an information system and do not keep them on the system itself.

Recommendation (Operational): Anti-virus protection

Define an antiviral policy that protect as priority equipment and applications in direct contact with the uncontrolled or unsafe environments. Perform a periodic audit and update of the protection mechanism. If you need to import external files or connect USB keys, systematically verify key is not infected with use of sanitization station.

Recommendation (Operational): Patch updates

Define a patch management policy (systematic, periodic or punctual) adapted to the functional constraints and identified risks. For example, define patch deployment priorities, verify backward compatibility and interoperability. Systematically apply patches to engineering stations and nomadic stations. Periodically apply patches on operator stations. Apply patches to sensitive installations during maintenance.

Recommendation (Operational): Protection of Programmable Logic Controller (PLC)

Protect access to the automatons with a password. Hardware offers the possibility of configuring read-only access for first level maintenance interventions. Protect access to source code and embedded code in CPUs. Disable remote configuration and/or programming modes when functionality exists. Lock the PLC cabinets with a key. On critical installations, install a dry contact when opening the cabinet.

Recommendation (Operational): Engineering stations and development stations

All of the above recommendations. Systematically apply the corrective measures. Always activate an antivirus. Do not connect nomadic consoles to networks other than SCADA networks. The consoles are nominative, or their use is traced. Switch off fixed stations when they are not in use and/or disconnect them from production networks.