Cyber Incident Sheets Industrial Control Systems

CLUSIF (French Information Security Club) – SCADA Working Group

April 2017

Thanks

CLUSIF wishes to celebrate the individuals who have made the creation of this document possible here, especially:

The managers of the working group:

Anthony	**Di Prima**	*Wavestone*
Hervé	**Schauer**	*HSC by Deloitte*

The contributors:

Christophe	**Auberger**	*Fortinet*	Patrice	**Bock**	*Sentryo*
Gaëtan	**Boin**	*Sogeti*	Jean	**Caire**	*RATP*
Loïc	**Guezo**	*TrendMicro*	Mathieu	**Hernandez**	*ENGIE Ineo*
Philippe	**Jeannin**	*RTE*	Guillaume	**Le Hegaret**	*Setec ITS*
Thierry	**Matusiak**	*IBM*	Thierry	**Pertus**	*Conix*
Philippe	**REBUFAT**	*Ministry of Defense*	Jérôme	**Richard**	*Econocom Digital Security*
Pascal	**Sitbon**	*Seclab*	Ilias	**Sidqui**	*Wavestone*

CLUSIF also thanks the members who have participated in the proofreading.

If you have any comments, please contact CLUSIF at the following address: scada@clusif.fr

Contents

Presentation of the "SCADA Security" Working Group

SCADA Working Group

- The SCADA working group is a group for dialogue and sharing between the information security stakeholders of the industrial world. It brings together ISSMs, architects, publishers and consultants.
- The aims of the CISOs group are to discuss practices in terms of cybersecurity solution providers and to analyze the current trends and industrial control systems.
- The group, created in 2013, undertook several works which ended up, among other things, in the publication of an overview of security benchmarks[1].
- In 2016, the working group studied the lessons to be learned from cases of incidents and attacks that took place on industrial systems with varying degrees of seriousness depending on the case.

[1] https://clusif.fr/publications/cybersecurite-des-systemes-industriels-par-ou-commencer-synthese-des-bonnes-pratiques-et-panorama-des-referentiels/

Presentation of the document

Aims

- The sheets presented in this document aim to raise awareness on cybersecurity in an industrial environment based on actual cases of attacks, incidents or proofs of concept for their educational dimension.

- In addition to information chief information security officers, the document is intended for a wider population, such as technicians, operators, system integrators, web developers, publishers, IT managers, operation managers and industrialists or branch heads, required to deal with this issue.

Approach adopted

1 Identification

Firstly, it was decided to **list** all of the incidents known to the members of the working group.

All of the research was open to **all of the business areas and all the countries.** Moreover, no time restriction was set.

The contributors identified a variety of attacks and cyber incidents.

The contribution was formed from **open, public sources.**

2 Selection

The incidents selected as the subject of a sheet had to respond to the following criteria:

- **Sufficient elements** available to describe the incidents, the unfolding of the attack and the impacts;
- **Multiple, consistent and verifiable sources** (magazines, information websites, reports coming from organisations);
- **A breach of an information control system** or **its surrounding environment, or an impact on industrial production or operation.**

3 Reproduction

The working group members divided up the writing of the incident sheets.

Each sheet is made up of 2 pages:

- **A visual** and an **overview description of the attack;**
- The **unfolding and the impacts** based on previously identified sources, as well as **CLUSIF recommendations.**

How do you interpret these sheets? 1/2

Presentation of the context of the attack:
- Year(s) over which the attack took place;
- Business area of the body affected;
- Place in which the body affected by the attack is located.

Title of the sheet

Brief description of the attack scenario or the incident and its impact

Illustrative visual of the incident

Vulnerability exploited to carry out the attack

How do you interpret these sheets? 2/2

The severity of the attack depends on the impacts noted. 4 levels of severity were identified:

- Low: little or no impact
- Average: temporary loss of production, no human impact, no ecological impact
- High: significant loss of production, injuries but no death, ecological impact
- Major: very significant financial and/or human impacts

A description of the unfolding of the attack based on the information collected and consolidated by the working group contributors.

Prise de contrôle d'un véhicule automobile

Club de la sécurité de l'information fra

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Sensibilisation	Élevée

Déroulement de l'attaque

- Certaines voitures sont équipées d'une option permettant au conducteur de **contrôler la console de bord par WiFi**. Les chercheurs ont réussi, en découvrant la clé Wifi, à s'introduire dans le réseau sans fil. Ils ont pris le contrôle de la console de bord en **exploitant ses vulnérabilités**.
- Les véhicules du même modèle sont connectés au réseau GSM. En utilisant une antenne GSM, les chercheurs ont réussi à **accéder à distance à la console de bord**.
- Cette console est connectée au CAN bus (réseau interne interconnectant les fonctions du véhicule), à travers un autre composant, le V850.
- En **modifiant le firmware** du V850, les chercheurs ont envoyé des commandes au véhicule.

Moyens m… en

- Deux personnes a… bonnes connaissan…
- Une antenne GSM … ebay
- Un nouveau firmware … reverse engineering

Enseignement à tirer, préconisation et contre-mesures

- Comme pour les SI industriels, les véhicules doivent **cloisonner les fonctions vitales / importantes de transport des fonctions de divertissement**. Les accès au… informatique du véhicule doivent être protégés :
  - La clé Wifi ne doit pouvoir être prédictible (date de sortie de l'usine)
  - Des mécanismes de contrôle d'accès doivent permettre de protéger les véhicules contre des actions non autorisées
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Utiliser un algorithme assurant une génération de clé non prédictible**
  - Mettre en place un **mécanisme empêchant la mise à jour du Firmware** du contrôleur V850 par un code non signé
  - Assurer un **filtrage des communications** entre le contrôleur V850 et le CAN bus (ACL, pare-feu…)

Fiche 13

2015	Transport	Saint Louis, USA	Wired

The complexity of the attack depends on the resources implemented. 4 levels of complexity were identified:

- Low: no tool required
- Average: tools required, technical skill easy for the attacker to acquire
- High: tools required, strong and specific technical skill
- Very High: specialized development for the attack with very significant financial and human resources

The conclusions to be drawn from this attack, as well as the messages to pass on are in this box.

Reminder of the context

What source(s) were used to create the sheet

Incidents analyzed

Energy

Sheet 1	Interruption in electricity production	France	2015
Sheet 2	General blackout - BlackEnergy	Ukraine	2015
Sheet 3	Data exfiltration from energy companies - Havex	Europe / USA	2013-2014
Sheet 4	Compromising of a computer network	Canada	2012

Oil & Gas

Sheet 5	Explosion of a pipeline	Turkey	2008
Sheet 6	Destruction of an information system - Shamoon	Saudi Arabia	2012
Sheet 7	Explosion of a gas pipeline	USSR	1982

Incidents analyzed

Water/sanitation

Sheet 8	Sewage treatment plant attack	Undisclosed	2015
Sheet 9	Putting a supervisory computer used to divert water out of commission	The USA	2007
Sheet 10	Discharge of waste water	Australia	2000
Sheet 11	Poisoning of drinking water	The USA	2013

Transport

Sheet 12	Taking control of tram switch	Poland	2008
Sheet 13	Taking control of a car	The USA	2015
Sheet 14	Disruption of rail signaling systems - Sobig/Blaster	The USA	2003

Incidents analyzed

Industry

Sheet 15	Denial of service in car factories - Zotob	The USA	2005
Sheet 16	Taking control of the manufacturing system of a steelworks	Germany	2014

Nuclear

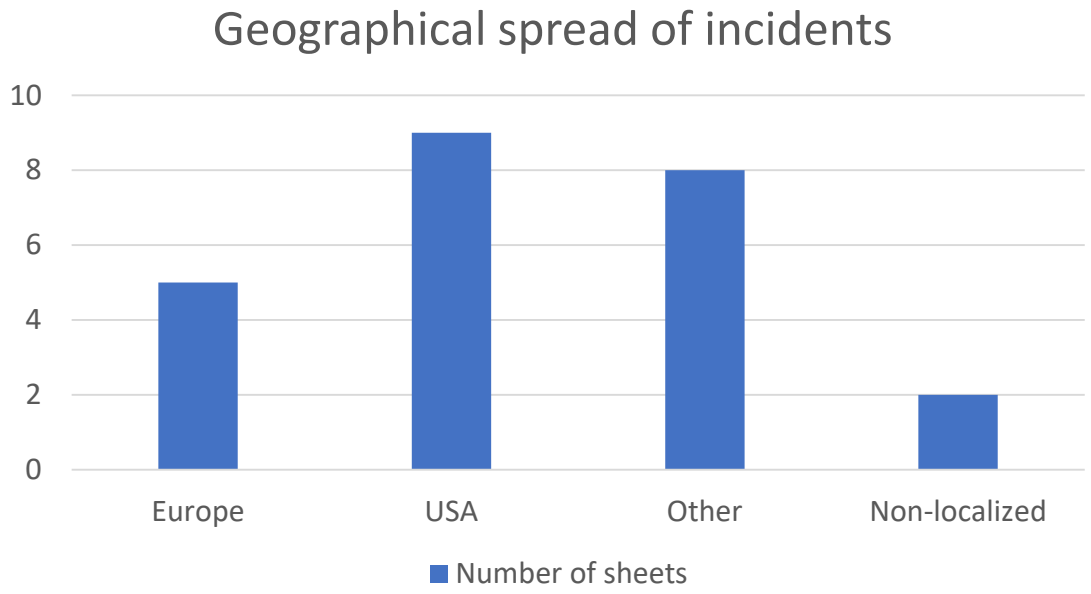
Sheet 17	Disclosure of documents from a nuclear power plant	South Korea	2014
Sheet 18	Sabotage of an industrial process - Stuxnet	Iran	2009-2010
Sheet 19	Worm infection in a nuclear power plant - Slammer	The USA	2003
Sheet 20	Emergency shutdown of a nuclear reactor	The USA	2008

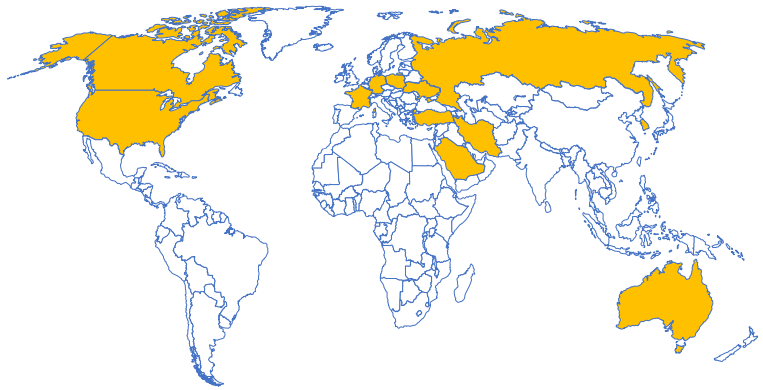
Other

Sheet 21	Diversion of a reconnaissance drone	Iran	2011
Sheet 22	Point of sale terminal attack - BlackPOS	The USA	2013
Sheet 23	Attack on an insulin pump	World	2011

Incident analysis

- The analysis of the geographical spread of incidents reveals several elements about the economic and regulatory situation of the countries. We note that:
  - **The countries the most affected are industrialized ones with an automated industry.**
  - **The country most represented in these sheets is the USA. This could be explained by the culture of transparency on these issues, with, moreover, regulations requiring companies to report certain incidents.**

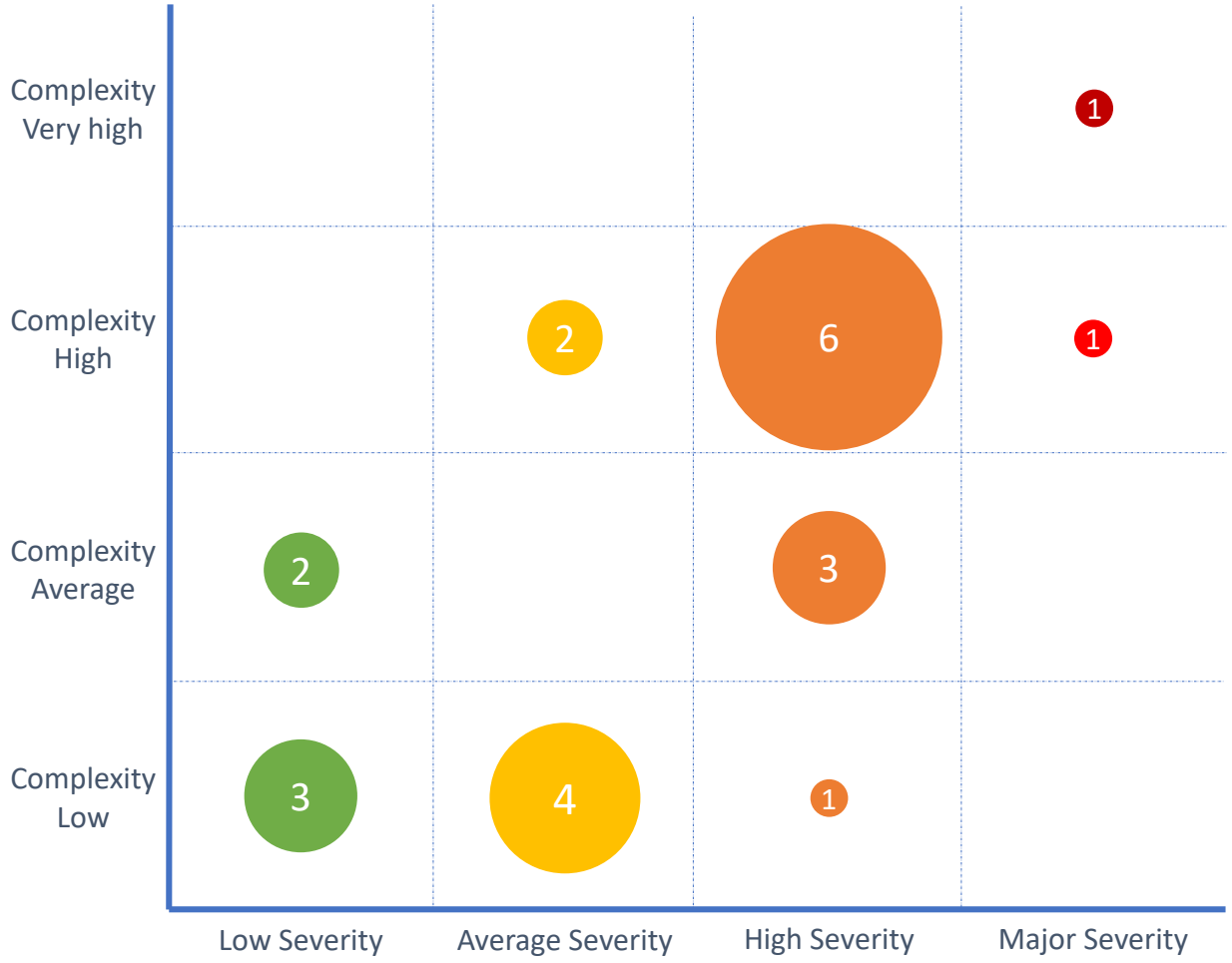




Incident analysis

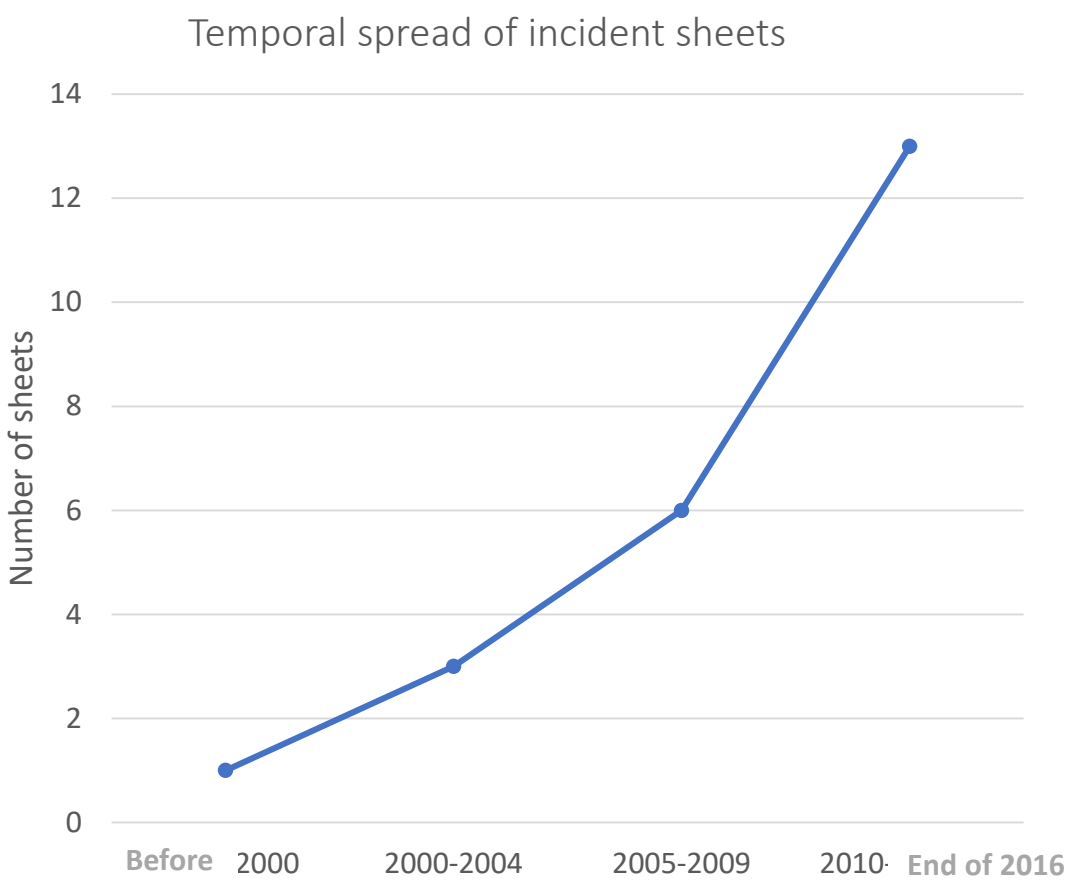
- The SCADA working group referenced attacks on industrial systems which were echoed in the press and security bodies, **whatever their severity.**
- The sheets were divided into **4 degrees of severity** (low, average, high and major). For each incident, the complexity of the attack was assessed according to **the public and available information.** The assessment of the complexity was done according to **4 levels** (low, average, high and very high).
- The cross analysis of the severity and complexity of attacks or incidents allows us to learn some lessons:
  - The very serious attacks have a high or even very high level of complexity: they are made possible if the attacker has **significant financial and material resources** and a **high level of expertise.** An attack on an industrial control system requires an in-depth knowledge of the field and the associated processes.
  - This knowledge can only be achieved when significant resources have been put in place to design the attack, for example, in the case of the attack on the power grid in Ukraine. This can, in part, explain why **there are still very few such attacks.**
  - The graph shows that **many low complexity attacks** were able to have **average or even high severity impacts.** This is a good illustration that **best practices in terms of security are not always applied in the systems.**

Number of sheets per severity/incidents



Incident analysis

- The incidents presented in this document represent one part of the attacks on industrial systems reported by the press or by security bodies.
- It is worth noting that, within the scope of this work, the attacks that had an impact on production systems or industrial information systems (or the surrounding network) have been **constantly increasing.** Several factors can explain this trend, which is being corroborated year after year, yet the most important is **the increased digital connectivity of industrial systems.**
- The **opening up** of industrial systems to technologies which were specific to the office area has made these systems **vulnerable to cyber attacks.**
- Furthermore, it was shown through the analysis of these different attacks that this transformation of industrial systems has not been matched by **adequate security measures. All the possible measures are detailed by the security benchmarks for which CLUSIF created an overview in 2014.** This overview is currently undergoing an update by the members of the SCADA working group, which is due to be published in 2017.



Overview

The incidents are increasing, with several causes:

- **The spread of information technology (IT) standards:** the majority of industrial protocols are currently on TCP/IP and an increasing amount of level 2 software (monitoring, logging, etc.), and even level 1 components (PLC, RTU, etc.) work on operating systems coming from the IT world.
- **The interconnection of industrial networks with office networks** targeting performance, reporting and savings.
- More generally, **the opening up to third party systems:** subcontracting of projects, remote obligations and outsourcing of maintenance, increase the access to industrial networks.

The main measures which would have been effective in view of this list of incidents are:

- **The control of logical** (networks) and **physical** (circulation of people, USB keys, portable PCs, etc.) **flows** within interconnections between the management information system and the industrial one, and within the industrial information system.
- **The control of external access** to industrial systems with strong authentication, local validation and isolation procedures in the event of an alert.
- **The monitoring of flows in order to detect attacks:** the most complex intrusions are preceded by recognition phases, the control by the operator of legitimate flows in his industrial network must be able to detect abnormal activities.

What are the trends for the coming years?

- The growing, yet moderate development in incidents reflects, in part, **the increase in the threat and vulnerability levels of** industrial information systems
- The "**democratization**" of attack softwares, like, for example, the publication of the Mirai[1] source code, allows stakeholders with limited resources to reuse these tools at a low cost: with each state attack (Stuxnet, Shamoon, Ukraine) there is a transfer of ideas or tools even. With the **emergence of industrial Internet of Things,** the massive introduction of smart items on the ground risks could lead to **increase the exposure level of industrial information systems considerably.** Their use in an urban context also introduces issues associated with **personal data protection** (until now restricted to management information systems).
- The **regulations** are being strengthened and now require a minimum level of cybersecurity for critical infrastructures, most of which are made up of industrial systems.
- States are equipping themselves with a **cyber arsenal** in order to be able to carry out operations in the cyber theater: **industrial systems being prime targets** in order to destabilize a state in view of the impacts that the attacks can cause.

Within this context, the challenge is to know if the awareness of the risk level and the security plans will be undertaken quickly enough and be sufficiently ambitious before serious incidents occur.
CLUSIF hopes to contribute to this via this set of "incident sheets".

[1] https://en.wikipedia.org/wiki/Mirai_(malware)

Incident sheets

Interruption in electricity production

2015 | Energy | Ouessant, France | Sheet 1

Impact

Cessation of electricity production for **15 days**

Incident scenario

Impossibility of accessing the communication system with the marine current turbine due to **ransomware**

Vulnerability

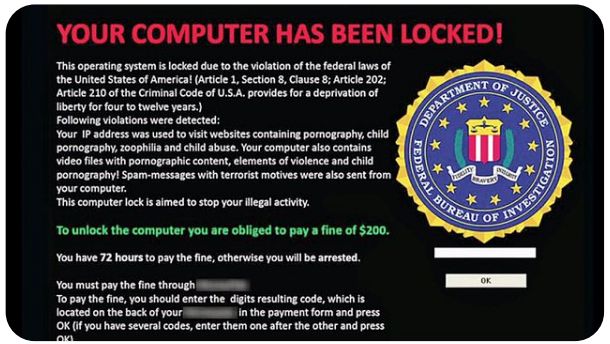
System's **direct connectivity** with the Internet without protection (absence of a firewall)

Interruption in electricity production

Severity of the attack	Motivation of the attacker	Complexity of the attack
Low	Financial	Low

Unfolding of the attack

- The attackers **encrypted the server** enabling a satellite connection with the control unit of the marine current turbine.
- They demanded **a ransom of $4000** be paid via PayPal or in Bitcoin so the connection could be reestablished.
- Sabella refused to pay, which lead to **an interruption of the system** during its test phase for 15 days.



Resources implemented

- Ransomware
- Internet connection

Lesson to learn, recommendation and countermeasures

- **Improving the control** and protection of **remote access systems** (strong authentication).
- The following measures would have been able to protect from it:
  - **Perimeter security:** Installation of a firewall, secure jump server
  - Implementation of a **redundant system** in order to ensure the continuity of production
- **Controlling the crisis communication:**
  - Avoid commenting about ongoing investigations in case you give incorrect information (attribution of the attack to Russian/Cuban hackers) risking negatively impacting on the the company's image (Sabella was still negotiating to develop new international markets)
  - Do not reveal the new protection resources implemented

2015	Energy	Ouessant, France	Ouest France, Usine Nouvelle

General blackout - BlackEnergy

2015 | Energy | Ivano-Frankivsk, Ukraine | Sheet 2

Impact

80,000 Ukrainian homes deprived of electricity, interruption from 3 to 6 hours

Incident scenario

Disconnection of substations from the grid via malware

Vulnerability

Naivety of users, lack of network segregation and control of authorizations

General blackout - BlackEnergy

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	Inter-state strategic	High

Unfolding of the attack

- A wave of « phishing » emails targeted 3 electricity utility companies. The email contained an infected Word file which, after it was opened and had its macros activated, installed the **BlackEnergy** malware on the desktop.
- To bypass the firewall separating the industrial information system from the management one, the attackers **hacked the active directory** and took control of the VPN accounts, allowing them to remotely control the SCADA.
- The attackers **reprogrammed the inverters** and corrupted the firmware of the serial to Ethernet gateways of the substations in order to disrupt the remediation operations.
- Finally, they launched the attack by **deactivating the inverters and the electrical substations.** They also launched a telephonic denial of service attack on the call center to stop users reporting the breakdowns.

Resources implemented

- A group of experienced individuals with a good understanding of industrial systems and very strong technical skills
- Malware (BlackEnergy)

Lesson to learn, recommendation and countermeasures

- The information system users must be made aware of the risk that spear phishing represents (campaign of infected emails). The formalization of **a business continuity plan** is able to reduce the impact (2 months after the attack, the affected distribution companies had still not returned to regular operations).
- The following measures would have been able to protect from it:
  - More significant **partitioning** of networks (use of a diode for example)
  - **Blocking of Office macros**
  - **Raising** employees' **awareness** on security
  - **Controlling** user **authorizations** (controlling write and firmware editing permissions)

2015 | Energy | Ukraine | Sillicon.fr, SANS

Data exfiltration from energy companies - Havex

2013-2014 | Energy | Europe and the USA | Sheet 3

Impact

Theft of data

Incident scenario

Penetration of internal energy company networks thanks to **malware inserted into software updates of three suppliers of SCADA industrial systems**

Vulnerability

Naivety of users, lack of test for software updates

Data exfiltration from energy companies - Havex

Severity of the attack	Motivation of the attacker	Complexity of the attack
Average	Espionage	High

Unfolding of the attack

- A group of hackers called Dragonfly used 3 different strategies to infect the computer networks of over 1000 companies from the energy sector:
  - Sending emails containing an **infected PDF** to senior executives of companies from the energy sector.
  - Compromising of websites associated with the energy sector with the effect of redirecting to harmful sites **responsible for infecting visitors via Trojan horses.**
  - Infection **of SCADA software updates of 3 suppliers** via free download on their website. Once they were updated, the control command systems therefore had backdoors useable by the group of hackers.

Resources implemented

- Trojan Horse (Karagany)
- Backdoor (Oldrea, Havex or Energetic Bear RAT)
- A group of individuals with very good technical skills (named Dragonfly or Energetic Bear)

Lesson to learn, recommendation and countermeasures

- The information system users must be made aware of the risk that **phishing** represents (sending of infected emails). Software updates, even when they come from publishers of solutions, can be corrupted.
- The following measures would have been able to protect from it:
  - **Raising** employees' **awareness** on security
  - Installation of computer **configuration change detection solutions** ("whitelisting") which will be able to detect the installation of backdoors
  - **Implementations of a software update testing process**

2013-2014	Energy	Europe and the USA	Symantec Report, BBC

Compromising of a computer network

2012 | Energy | Canada | Sheet 4

Impact

Logging out of customer remote access

Incident scenario

Theft of customer data (NOC remote access passwords) and theft of information concerning their OASyS SCADA product

Vulnerability

Bypassing of firewalls

Compromising of a computer network

Severity of the attack	Motivation of the attacker	Complexity of the attack
Average	Espionage	High

Unfolding of the attack

- Telvent is a company which designs SCADA software.
- The group of Chinese hackers was able to infect the Telvent network by bypassing an **internal firewall.**
- The attackers were targeting the OASyS SCADA software and were aiming to modify customer files.
- The attackers succeeded in gaining access to the management information system of Telvent.
- If they had been able to see their attack through, they would have been able to modify the SCADA software code.
- After having noticed the attack, **Telvent informed its customers and cut all connections with them.**

Resources implemented

- Group of Chinese hackers bearing the name *Comment Group*

Lesson to learn, recommendation and countermeasures

- The companies developing software for industrial information systems must **protect the development environments** and ensure that they are **partitioned from the rest of the information system.**
- The following measures would have been able to protect from it:
  - **Raising employees' awareness on security**
  - **Partitioning of the development environments**

- Positive point: Although it was not legally required to do so, **Telvent informed its customers about the attack.**

2012 | Energy | Canada | Canada.com, automationworld

Explosion of a pipeline

2008 | Oil & Gas | Turkey | Sheet 5

Computer origin of the incident contested

Impact

Destruction of the Baku-Tbilisi-Ceyhan (BTC) pipeline, Destruction of equipment, unavailable for 20 days (over **$1 billion** of loses in equipment and revenue)

Incident scenario

Deactivation of monitoring systems and **alarms** then explosion

Vulnerability

Camera software, access to valves, radio network exposed

Explosion of a pipeline

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	Inter-state strategic	High

Unfolding of the attack

- The surveillance cameras installed along the pipeline were vulnerable and connected to the monitoring center via the Internet. By exploiting these vulnerabilities, the attackers were able to access the alarm management server (which was also vulnerable) in the center. They deactivated the safety alarms and the communication means of local teams (by interfering with the wireless communication).
- By going for a pumping station, the attackers manipulated the industrial systems (industrial and automated stations) causing a rise in the pressure within the pipeline and its explosion.
- The pipeline monitoring center was aware of the explosion 40 minutes after it took place thanks to a warning raised by a technician on the premises when the incident occurred.

Resources implemented

- Combined physical and cyber attack
- Deactivation of surveillance cameras and alarms
- Manipulation of industrial systems

Lesson to learn, recommendation and countermeasures

- **Checking the availability of surveillance resources** is required to ensure the cybersecurity of the industrial information system. The absence of a response from an alarm system is an incident in itself. Furthermore, the **security of physical access** is a vital parameter in the security of industrial information systems.
- The following measures would have been able to protect from it:
  - **Diversification of surveillance resources**
  - **Hardening of industrial systems** and of **physical access controls**
  - **Partitioning of systems**
  - **Maintenance of security equipment** (e.g.: vulnerable cameras and server)

2008 | Oil & Gas | Turkey | Bloomberg

Destruction of an information system - Shamoon

2012 | Oil & Gas | Dhahran, Saudi Arabia | Sheet 6

Impact

Inability to supply customers, **partial invoicing, recovery after 5 months**

Incident scenario

Total or partial destruction and deletion of files of **30,000 workstations and 2,000 servers**

Vulnerability

Lack of employee awareness

Destruction of an information system - Shamoon

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	Political	Average

Unfolding of the attack

- An employee from the company with a privileged account probably clicked on a link contained in a SCAM message (**phishing**).
- The **Shamoon virus** was quickly deployed over the whole network of **30,000 workstations and 2,000 servers.**
- The virus exfiltered the files from workstations and servers, then deleted them. Then, the virus destroyed the machines **by rewriting the** disc **boot sector.**
- The core business was affected: management of orders, stock, supply, invoicing, etc. Only the oil extraction was not affected (officially, SCADA network separate).

Resources implemented

- Shamoon virus
- Low financial investment
- No specific equipment

Lesson to learn, recommendation and countermeasures

- The **raising of** user **awareness** remains an important point to take into consideration.
- Flat networks allow malware to spread very easily.
- The following measures would have been able to protect from it or limit its impact:
  - Implementing of an **intrusion detection system**
  - Segmenting the network by sensitivity level
  - **Raising** employees' **awareness** on security
  - Implementing **a business continuity plan** by specifying the use of spare equipment

2012 | Oil & Gas | Saudi Arabia | CNN, NY times

Explosion of a gas pipeline

1982 | Oil & Gas | USSR | Sheet 7

Origin of the incident contested

Impact

Explosion of the pipeline of Urengoy–Pomary–Uzhgorod, no victims

Incident scenario

Over-pressurization in the pipeline caused by a Trojan horse and a logic bomb

Vulnerability

Bugged software stolen by the KGB from a Canadian firm

Explosion of a gas pipeline

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	Inter-state strategic	High

Unfolding of the attack

- Thanks to documents disclosed by a double agent from the CIA who infiltrated the ranks of the KGB ("Farewell Dossiers"), the CIA was aware of the mass technology theft by the USSR (Line X).
- The CIA had therefore bugged its technology (including the software) in order to retaliate against the USSR and discredit the already stolen technology.

Resources implemented

- State strategy
- High confidentiality
- Modification of software code

Lesson to learn, recommendation and countermeasures

- A piece of software or a technology may **contain Trojan horses, back doors,** etc.
- The following measures would have been able to protect from it:
  - **Audit of the software source code**
  - **Installation of security mechanisms independent of the information system** (e.g.: safety systems)

2012 | Oil & Gas | USSR | At the Abyss: An insider's History of the Cold war (ISBN 0-89141-821-0)

Waste water treatment plant attack

2015 | Water / Sanitation | Location not disclosed | Sheet 8

Impact

Disruption of water treatment process

Incident scenario

Modification of the doses of chemical products used for water treatment

Vulnerability

Vulnerability in an online **application** connected to the industrial system

Waste water treatment plant attack

Severity of the attack	Motivation of the attacker	Complexity of the attack
Low	Fraud	Low

Unfolding of the attack

- The attacker took **control of the online payment application** in order to steal customer data.
- The server executing this application (an AS400) was hosting **the login data of an administrator account** as well **as the IP address of the server** managing the industrial process. By using this data the attacker had **access to the control interface of the installation.**
- The attacker modified the parameters of the application, leading to a disruption in the waste water treatment process.
- The disruptions were limited thanks to the responsiveness of the industrial teams who reestablished the proper working of the industrial process thanks to **their discussions** with the IT teams.

Resources implemented

- Basic hacking tools (SQL injection)
- Very little knowledge of SCADA systems
- No particular knowledge of the operation of the industrial process

Lesson to learn, recommendation and countermeasures

- **The absence of control between the industrial system and the online payment system**, the **weak authentication level** and the **poor protection of passwords** made the industrial system vulnerable to attacks coming from the Internet.
- The following measures would have been able to protect from it:
  - **Segregation** between the industrial information system and the management one
  - Implementation of **strong authentication** for accessing industrial systems
  - Conducting of **recurrent audits** for applications exposed to the Internet to identify the known vulnerabilities
- Positive point: **Safety system, discussions** between the IT and industrial teams following suspect behavior.

2015	Water / Sanitation	Location not disclosed	Verizon report, The register

Putting a supervisory computer used to divert water out of commission

2007 | Water / Sanitation | Willows, USA | Sheet 9

Impact

Denial of service to the supervisory computer / **$5000 in damages**

Incident scenario

Dismissed employee damaged the supervisory computer

Vulnerability

Lack of monitoring of employee access rights

Putting a supervisory computer used to divert water out of commission

Severity of the attack	Motivation of the attacker	Complexity of the attack
Low	Revenge	Low

Unfolding of the attack

- A **former employee** of the Tehama Colusa Canal Authority intentionally installed **unauthorized software** on the computer responsible for diverting the water from the Sacramento river for irrigation purposes.
- The installation of this software **damaged the computer** that was a part of the SCADA.
- The operators therefore switched to manual control.

Resources implemented

- A single individual with limited knowledge
- Low financial investment
- Unrestricted access to the supervisory computer

Lesson to learn, recommendation and countermeasures

- It is important not to overlook the **threats coming from inside** of the company (discontented employee, handling errors, etc.).
- The following measures would have been able to protect from it:
  - **Limiting users' rights**
  - **A procedure to revoke employee rights** (departure, changing of role, transfer)
  - **Monitoring** of the change in the supervisory computer's configuration
- Positive point: The operators still had the option of switching to **manual control** reducing the damage cased by this incident.

2007	Water / Sanitation	Willows, USA	Computer world

Discharge of waste water

2000 | Water / Sanitation | Maroochy, Australia | Sheet 10

Impact

800 m^3 of waste water discharged into rivers and parks

Incident scenario

Control taken remotely by a rejected applicant

Vulnerability

Remote access radio network without authentication

Discharge of waste water

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	Revenge	Low

Unfolding of the attack

- An ex-employee from the company which installed the SCADA system of the sewage treatment plant of Maroochy Shire applied for a position within the company.
- His application was rejected so he decided **to take revenge** on the 2 employers by taking control of the plant. He therefore **stole a radio device from his employer** and sent commands to the control system that he helped to install.
- The command sent allowed him to discharge hundreds of thousands of liters of waste water.
- **His understanding of the industrial process** allowed him to pretend that his actions were due to a system malfunction.

Resources implemented

- A single individual with technical and industrial process knowledge
- Low financial investment
- A stolen radio device

Lesson to learn, recommendation and countermeasures

- **The supervision of devices** as well as access rights is an integral part of security.
- The use of an unencrypted transmitted protocol even if it is proprietary does not protect against attacks.
- The following measures would have been able to protect from it:
  - **Anti-replay mechanisms** to avoid simple attacks aiming to replay commands or legitimate operations
  - **Monitoring** to trace back the history of events and incident management procedures
  - Implementation of an **authorization and device control** process
  - **Raising employee's awareness** to distinguish malfunctions from cases of actual attacks.

2000	Water / Sanitation	Maroochy, Australia	The Register, NIST Report

Poisoning of drinking water

2013 | Water / Sanitation | Georgia, USA | Sheet 11

Impact

400 residents deprived of water

Incident scenario

Modification of fluorine and chlorine ratio settings

Vulnerability

Lack of monitoring of installation. Physical access possible without raising the alarm

Poisoning of drinking water

Severity of the attack	Motivation of the attacker	Complexity of the attack
Average	Revenge?	Low

Unfolding of the attack

- The attackers entered the plant **by going over the barbwire.**
- No breaking in at the doors or windows.
- The attackers had access to the **monitoring system** and **modified** the fluorine and chlorine ratio **settings**.
- The vehicles of employees have GPS and show that none of them were near the plant during the incident.
- The management company of the plant informed the population of the attack.

Resources implemented

- One or several individuals with knowledge of the plant
- No financial investment

Lesson to learn, recommendation and countermeasures

- The **security of physical access** is a parameter to take into consideration when securing industrial information systems.
- The following measures would have been able to protect from it:
  - Strengthened **control of physical access**
  - **Monitoring of at risk areas**
  - **Revoking of access when an employee leaves**
  - **Monitoring of security**

2013 | Water / Sanitation | USA | wrcbtv.com

Taking control of tram switch

2008 | Transport | Lodz, Poland | Sheet 12

Impact

4 trams derailed, 12 people with minor injuries

Incident scenario

The switch system was **taken control** of by a teenager

Vulnerability

Radio network without authentication

Taking control of tram switch

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	Fun / For challenge	Average

Unfolding of the attack

- In the city of Lodz in Poland, a teenager infiltrated the tram depot of the city and **studied the network**, as well as the trams for **a long period.**
- He therefore modified a **TV remote** in order to allow him to alter the switches of the tram network.
- Without realizing his actions, the teenager derailed 4 trams by modifying the switch injuring 12 people.

Resources implemented

- A single person with knowledge of an academic level
- Low financial investment
- A modified TV remote

Lesson to learn, recommendation and countermeasures

- The use of an **unencrypted** transmitted protocol even if it is proprietary does not protect against attacks.
- The following measures would have been able to protect from it:
  - **Mutual authentication** to ensure that only authorized devices can communicate with the switch system
  - **Anti-replay mechanisms** to avoid simple attacks aiming to replay commands or legitimate operations
  - **Encryption of flows** to stop the analysis of signals and man-in-the-middle type attacks

Taking control of a motor vehicle

2015 | Transport | Saint Louis, USA | Sheet 13

Proof of concept

Impact

Taking control of a vehicle, obligation to recall vehicles (1.4 million vehicles)

Incident scenario

Vehicle taken control of by two researchers

Vulnerability

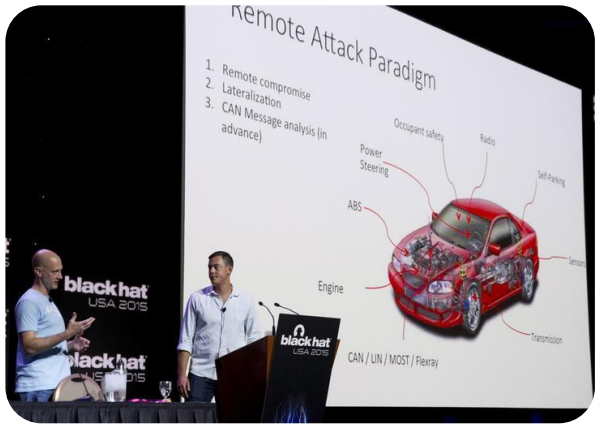
WiFi network with predictable key and **vulnerabilities of a controller attached to the CAN bus** (internal network interconnecting the vehicle functions)

Taking control of a motor vehicle

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	Awareness raising	High

Unfolding of the attack

- Some cars are equipped with an option allowing the driver to **control the dashboard via WiFi.** Researchers succeeded in accessing the wireless network, by discovering the WiFi key. They took control of the dashboard by **exploiting its vulnerabilities.**
- The vehicles of the same model are connected to the GSM network. By using a GSM antenna, the researchers succeeded in **remotely accessing the dashboard.**
- This console is connected to the CAN bus (internal network interconnecting the vehicle functions), via another component, the V850.
- By **modifying the firmware** of the V850, the researchers sent commands to the vehicle.



Resources implemented

- Two people with very good technical skills
- A GSM antenna bought on eBay
- A new firmware created by reverse engineering

Lesson to learn, recommendation and countermeasures

- As with industrial information systems, vehicles must **segregate vital / important transportation functions from leisure functions.** The access to the computer system of the vehicle must be protected:
  - The WiFi key must not be predictable (date the car left the factory)
  - Access control mechanisms must be able to protect vehicles against unauthorized actions
- The following measures would have been able to protect from it:
  - **Using an algorithm ensuring non-predictable key generation**
  - Implementing a **mechanism stopping the Firmware update** of the V850 controller by an unsigned code
  - Ensuring **communication filtering** between the V850 controller and the CAN bus (ACL, firewall, etc.)

2015 | Transport | Saint Louis, USA | Wired

Disruption of rail signaling systems -SoBig & Blaster

2003 | Transport | United States of America | Sheet 14

Impact

Disruption of rail traffic for a day in the East of the United States

Incident scenario

Simultaneous attack from two viruses (SoBig.F and Blaster) on the control systems of CSX Corporation (American rail company) causing them to be rendered unavailable

Vulnerability

Security holes in Windows, virus not detected by anti-virus, use of scam emails

Disruption of rail signaling systems -SoBig & Blaster

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	Fun	Average

Unfolding of the attack

- The control system was infected by viruses, leading to the slowing then **stopping of rail control, signaling and communication applications.**
- The train traffic was disrupted
- The neutralization then restarting of services was, however, quick (a day)

Resources implemented

•The SoBig virus spread between 2002 and 2003 by exploiting a security hole in Windows and via using scam mails

•The Blaster virus spread in 2003 and generated denial of service attacks

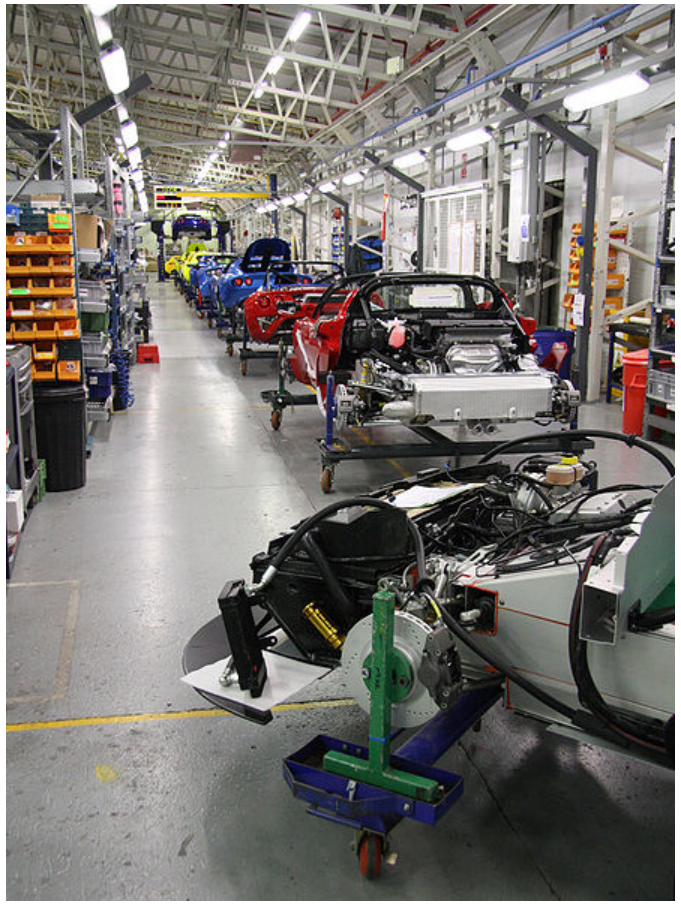
•Low financial investment

Lesson to learn, recommendation and countermeasures

- The following measures would have been able to protect from it or limits its impact:
  - **Awareness raising** of users on scam emails and propagation techniques, use of anti-virus to check the attachment of emails
  - **Updating anti-virus databases**
  - Neutralization of infected servers by telecommunication operators or by hosts
  - **Securing of office applications** (Office, etc.) to limit any attempt to spread the virus

Denial of service in car factories - Zotob

2005 | Industry | United States of America | Sheet 15



Impact

13 factories shutdown for 1 hour, 50,000 workers ($14M in damages)

Incident scenario

Propagation of a worm in the assembly chain

Vulnerability

Lack of filtering at the level of the interconnection of the industrial network with the office network

Denial of service in car factories - Zotob

Severity of the attack	Motivation of the attacker	Complexity of the attack
Average	Indiscriminate attack	Low

Unfolding of the attack

- The **Zotob** worm, discovered in 2005, spread over the Internet by exploiting vulnerabilities present in the PnP protocol. The systems affected by this work are networked Windows machines (un-patched Windows 2000 ones in particular).
- The Windows 2000 servers of DaimlerChrysler were victims of this infection wave.
- Despite a **firewall** between the company and industrial networks, the worm found its way into **the industrial systems.** It **spread between the factories,** making them unavailable.

Resources implemented

- A worm (Zotob)
- Services exposed to the outside
- Interconnected networks

Lesson to learn, recommendation and countermeasures

- A critical system must be sufficiently **partitioned** to limit the spread of attacks.
- The following measures would have been able to protect from it:
  - **In-depth defense** and **strict segregation** of the systems linked to production (physical isolation, diode, hardware protection)
  - **Limiting of services exposed to the outside**: hardening of systems, filtering of authorized flows

2005 | Industry | USA | eWeek

Taking control of the manufacturing system of a steelworks

2014 | Industry | Germany | Sheet 16

Impact

Significant physical damage caused by the loss of control of manufacturing software

Incident scenario

The factory's control system was taken over by **spear phishing** via the office network

Vulnerability

Gateway between the manufacturing network and the office network

Taking control of the manufacturing system of a steelworks

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	Financial or Terrorist	High

Unfolding of the attack

- The hackers firstly entered the office network of the industrial site via the **spear phishing** technique (campaign of infected emails).
- From this first network, they penetrated the manufacturing management software of the steelworks, then took control of the majority of the factory's control systems.
- They therefore stopped a blast furnace from being secured in time and caused serious damage to the infrastructure.

Resources implemented

- A group of experienced individuals with a good understanding of industrial systems
- Significant financial investment

Lesson to learn, recommendation and countermeasures

- The attack method via spear phishing required significant means and good understanding of targeted systems, but proved to be undeniably effective.
- The following measures would have been able to protect from it or limit its impact:
  - **Awareness raising** of workers and users in the attack methods via spear phishing
  - **Restriction of rights granted to user profile** on the network and systems, in order to detect or stop any suspect action (taking control of systems, terminals, etc.)
  - **Partitioning of** office **networks**, exposed to attacks and intrusions, and control networks of manufacturing systems
  - Implementation of safety mechanisms **independent** of the control system

2014 | Industry | Germany | BSI, Arstechnica

Disclosure of documents from a nuclear power plant

Impact

Publication of technical documentation on reactors and **information on staff** of KHNP (Korea Hydro & Nuclear Power)

Incident scenario

Infection of accounts of KHNP employees

Vulnerability

Staff negligence

Disclosure of documents from a nuclear power plant

Severity of the attack	Motivation of the attacker	Complexity of the attack
Low	Political / Financial	Average

Unfolding of the attack

- After a **spear phishing campaign** (campaign of infected emails) which affected **3,571 employees,** the attacker was able to gain access to the different KHNP documents.
- The attacker **published documents on Twitter** on several occasions, pretending to be the vice president of an anti-nuclear association and advised people living near to plants to leave the areas.
- The attacker also asked for **a ransom** to not publish the documents.
- It would appear that the attacker had **tried to attack the industrial system** but did not succeed.

Resources implemented

- Targeted phishing campaign
- Kimsuky is malware supposedly used by North Korea

Lesson to learn, recommendation and countermeasures

- The employees were not sufficiently **aware** of the different threats and attacks via "spear phishing".
- The following measures would have been able to protect from it:
  - Carrying out an **awareness raising campaign**
  - **Classifying information** on the company
  - Adapting the security level according to the **level of data confidentiality** (Encryption, access restriction & traceability)
- Positive point: After the attack, KHNP undertook **an exercise** to check its capacity to face a cyber attack.

Sabotage of an industrial process - Stuxnet

2009-2010 | Nuclear | Natanz, Iran | Sheet 18

Impact

Delay of **6 months to 1 year** in the Iranian nuclear program, **several million euros** of equipment damaged (mainly in the Natanz plant)

Incident scenario

Advanced malware (called **Stuxnet**), injected into a management information system workstation which spread all the way to the industrial information system

Vulnerability

Absence of USB key control, no segmentation or intrusion detection in the industrial information system, **PCs not hardened**, industrial equipment with **ignored vulnerabilities**

Sabotage of an industrial process - Stuxnet

Severity of the attack	Motivation of the attacker	Complexity of the attack
Major	Inter-state strategic	Very high

Unfolding of the attack

- After a significant **espionage stage** of the Iranian nuclear facilities and significant **research and development** work, the attackers succeeded in developing the **Stuxnet** virus.
- Stuxnet was able to **replicate itself and circulate without a harmful effect,** until the target (centrifuge control and command system).
- Once it reached the management information system, it was able to spread to the industrial information system, **even in the absence of a network interconnection** (via USB or laptop).
- The "active load" (logic controller code) was very complex, derailing the process in a way that was **not very detectable,** with the consequence of prematurely wearing the centrifuges, mechanical components, very sensitive to certain resonance frequencies. This load was not activated until it was in contact with the logic controller.

Resources implemented

Organization commissioned by the USA in partnership with Israel:

- "Software engineering" workshop dedicated to the development of Stuxnet:
  - 15 exploits
  - 4 0-day
- Espionage
- Internal local collusion

Lesson to learn, recommendation and countermeasures

- Protection via **network isolation** ("air-gap") is not effective. Furthermore, the attack was revealing as to the **attack capabilities of a state.**
- The following measures would have been able to protect from it:
  - **Protection of information** (architecture & codes) on industrial processes.
  - Consideration of cybersecurity demands during the **design of industrial equipment and applications.** They contain a great deal of "flaws", often without a solution.
  - **Development of all the defense areas:** segmentation (networks, rights, info), detection, hardening, vulnerability management, etc.

2009 | Nuclear | Natanz, Iran | Ralph Langer Blog, NY Times

Worm infection in a nuclear power plant - Slammer

2003 | Nuclear | Ohio, USA | Sheet 19

Impact

Davis-Besse plant unavailable for 6 hours, safety systems ineffective

Incident scenario

Propagation of a worm via a private communication network

Vulnerability

Interconnection between a private communication network and the industrial systems

Worm infection in a nuclear power plant - Slammer

Severity of the attack	Motivation of the attacker	Complexity of the attack
Average	Indiscriminate attack	Low

Unfolding of the attack

- During January 2003, the Slammer worm infected several Microsoft SQL 2000 servers over the world therefore causing a significant **denial of service**.
- Initially, the worm had infected the server of a service provider of the plant. This workstation had a T1 type connection linking it directly to the industrial information system **bypassing the firewall** separating it from the management information system.
- The worm therefore sent several packets on the industrial network **overloading** it and **therefore rendering the safety system** (safety parameter display system (SPDS)) and the plant control workstation **unavailable.**

Resources implemented

- A worm (Slammer)
- Services exposed to the outside
- Interconnected networks

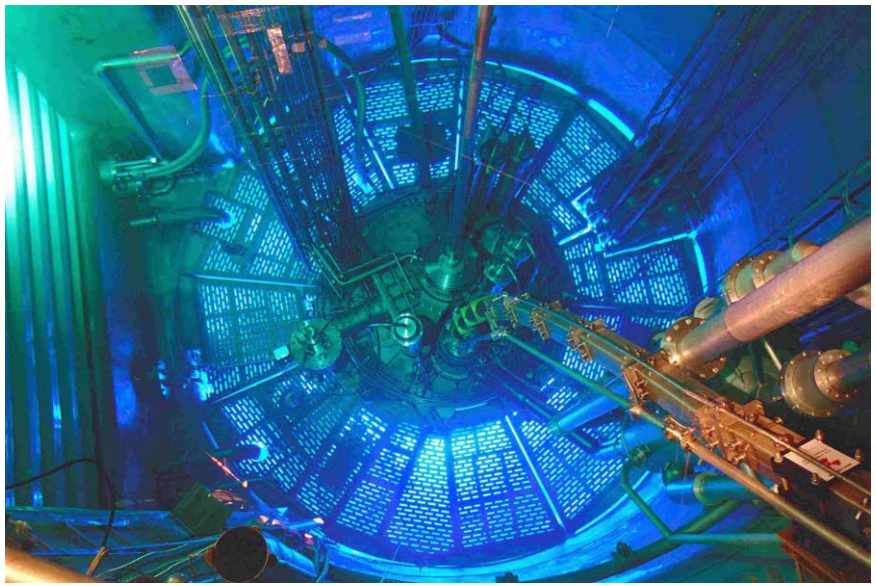
Lesson to learn, recommendation and countermeasures

- An understanding of the different existing interconnections between the industrial network, the management information system and the external networks was required to implement the appropriate defense infrastructures.
- The following measures would have been able to protect from it:
  - **Mapping of the information system** with a strict partitioning of the industrial network and of the systems linked to safety (physical isolation, diode & hardware protection)
  - **Limiting of services exposed to the outside**: hardening of systems, filtering of authorized flows
  - **Application of security patches**

2003 | Nuclear | Ohio, USA | Security Focus

Emergency shutdown of a nuclear reactor

2008 | Nuclear | Hatch, Georgia, USA | Sheet 20



Impact

Shutdown of a nuclear reactor

Incident scenario

An update resets the data from the control system

Vulnerability

Poor integration of "Commercial Off-The-Shelf" (COTS) components with industrial control systems

Emergency shutdown of a nuclear reactor

Severity	Motivation	Complexity
Average	Error	Low

Unfolding of the attack

- An engineer installed an update of a software present on a workstation of the management information system of the plant. This workstation was able to analyze the data sent by the SCADA. **The update was designed to synchronize the two information systems.**
- After the update, **the restart of the system reset the data of the control system.**
- The safety measures interpreted the erroneous data and concluded that it was a leak from the "pool".
- The nuclear reactor went into emergency shutdown.

Resources implemented

- A single person in charge of SCADA monitoring interfaces
- Inappropriate or poorly integrated software
- Unsecured procedures

Lesson to learn, recommendation and countermeasures

- When the networks are poorly partitioned, **a legitimate update of systems can place the industrial information system in danger.**
- The following measures would have been able to protect from it:
  - Establishment of a **software update protocol**
  - **Partitioning of the critical industrial information system,** and particularly the data servers
  - **Communication with the software publishers** to determine the possible repercussions that a software update of the information system may have.
  - **Carrying out of update tests** on systems outside of production before they are applied to production

2008 | Nuclear | USA | Washington Post

Hijack of a reconnaissance drone

2011 | Defense | Iran | Sheet 21

Impact

Recovery of an American "Sentinel" **drone** allowing for retro-engineering and copying

Incident scenario

Hijack via **false GPS signal transmission** deceiving the drone, but also remote control

Vulnerability

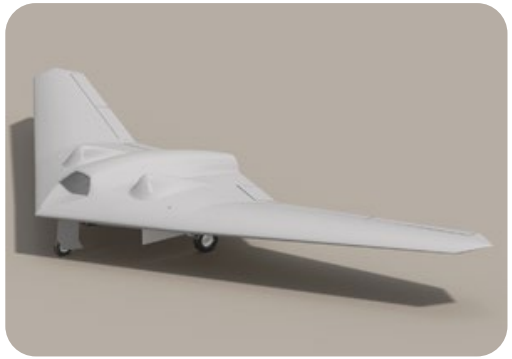
Lack of GPS system securing

Diversion of a reconnaissance drone

Severity of the attack	Motivation of the attacker	Complexity of the attack
High	(plans, etc.)	High

Unfolding of the attack

- Analysis of the way navigation and remote piloting work for older drones (damaged).
- Attack in two stages, once a drone is in the scope of the transmitters:
  - **Interference of communication** for remote piloting: the drone switches to "auto-pilot" mode and will land at its base
  - **Modification of the GPS signal** so that its "base" coincides with a runway on Iranian territory.



Resources implemented

- Retro-engineering of drones.
- Communication interference and transmission of false GPS signals with enough power to deceive a drone in flight.

Lesson to learn, recommendation and countermeasures

- The **vulnerability was known** to the American army (according to Christian Science Monitor) and the risk poorly assessed (or not identified): **risk management** based on identification of vulnerabilities is essential.
- The GPS signal must be considered as **unreliable** for critical applications.
- Cybersecurity must be considered in the degraded modes of control systems.

2011 | Defense | Iran | Linformaticien, csmonitor

Point of sale terminal attack - BlackPOS

2013 | Distribution | United States of America | Sheet 22

Impact

40 million bank card numbers hijacked, **70 million Target** (mass retail chain) **customer accounts pirated,** stock market devaluation, dismissal of the CEO

Incident scenario

Compromising of point of sale terminals by a **Trojan horse**

Vulnerability

Unprotected remote access for air conditioning maintenance

Point of sale terminal attack - BlackPOS

Severity of the attack	Motivation of the attacker	Complexity of the attack
Major	Financial	High

Unfolding of the attack

- The attackers launched a targeted attack to collect the connection settings (username/password) of the **remote access of an air conditioning system maintenance service provider.**
- **They were therefore able to access the PoS** (Points of sale) **via bouncing off the industrial network,** in order **to install the malware** (BlackPOS) to intercept **the bank card codes on the fly.** The malware was responsible for placing this data **on an internal compromised server.**
- Finally, **the banking data** collected beforehand was exfiltered to a **external FTP server** (located in Russia) before being sold online.

Resources implemented

- Social engineering via email with infected attachment (*spear phishing*)
- Use of BlackPOS malware, RAM-scraping type (Trojan)

Lesson to learn, recommendation and countermeasures

- The global **governance** of the company's cybersecurity must incorporate **the technical management of buildings.**
- The following measures would have been able to protect from it:
  - Implementation of effective protection beyond simple compliance with regulations (Target had just been PCI-DSS certified)
  - Implementation of **strong authentication** in terms of remote access (standard access on the external invoicing system)
  - Implementation of **network partitioning** in order to protect the sensitive areas (horizontal placement up to the industrial network)
  - Implementation of **technical monitoring** of flaws discovered in the PoS (warning report published by Visa several months beforehand)
  - Implementation of **cyber monitoring of the information system** aiming to manage the alerts coming from detection measures (FireEye alerts ignored)

2013 | Distribution | USA | American Senate Report: A kill chain analysis

Attack on an insulin pump

2011 | Health | World | Sheet 23

Proof of concept

Impact

Potential modification of insulin doses

Incident scenario

Alteration and sending of radio commands

Vulnerability

Data unencrypted and lack of sensor authentication

Attack on an insulin pump

Severity of the attack	Motivation of the attacker	Complexity of the attack
Low	Awareness raising	Average

Unfolding of the attack

- After analysis of the manufacturer's documentation (user guide, analysis of patents, series number of the device, etc.) a researcher was able to **intercept the communications** exchanged between the sensors and his insulin pump.
- The analysis of logs showed that the pump was using, among others, a **non-obfuscated** JAVA application which controlled the equipment. The researcher was therefore able to establish the list of **useful command codes of the device.**
- The researcher imagined several attack scenarios: **replay** of values transmitted to the pump via the sensors, **sending of forged commands** directly to the pump (physical access required to know the series number required for sending).

Resources implemented

- Radio antenna (for less than €100 on eBay).
- Knowledge of the tools and "radio" technology

Lesson to learn, recommendation and countermeasures

- Smart objects present several vulnerabilities associated with the **lack of integration of security during their design.** Furthermore, autonomous devices **do not have a safety system** like in traditional industrial systems, making an attack potentially more dangerous.
- The following measures are able to secure this kind of health devices:
  - Requiring **mutual authentication** of sensors and insulin pumps;
  - **Encrypting** exchange signals;
  - In conclusion: integrating **security into the design stage** of these items.

Presentation of CLUSIF

Presentation of CLUSIF

- A not-for-profit association bringing together security professionals
  - **Over 250 member companies**
  - **15 economic sectors represented**
  - **Providers and users brought together in a balanced way**

- Discussing and acting together in favor of confidence in digital
  - **Creating and delivering a set of best practice in terms of information security via:**
    - Working groups
    - Publications
    - Themed conferences

The association's activities

- Working groups
  - **Monthly meeting of users and providers around given issues**
  - **Aiming to create then publish a white paper, best practice guide, recommendations or state of the art type document**

- Publications
  - **Provision (for free) of all of the documents produced by the association's working groups on the CLUSIF website**

- Conferences
  - **5 themed conferences per year to raise awareness on the importance of information security**

A space dedicated to CISOs

- The CLUSIF CISO Space, a special place for dialogue
  - **Reserved for information system security managers from private companies and the public sector (excluding providers of security solutions or services)**
  - **Favors the exchanging of expertise and feedback on:**
    - Issues encountered
    - Solutions implemented
    - New standards
    - New regulations and legal requirements
  - **One-off talks from institutional bodies**
  - **Monthly meetings, generally on Friday at the start of each month**

For more information

- Association's website
  www.clusif.fr

- Club de la sécurité de l'information
  11 rue de Mogador
  75009 Paris
  clusif@clusif.fr

Photo credits

Photo credits

Overview:

- http://www.mintincorp.com/industrial-sector/oil-gas/

Interruption in electricity production - slide 1:

- https://upload.wikimedia.org/wikipedia/commons/4/42/Hydrolienne_Sabella_D10_%284%29.JPG

Interruption in electricity production - slide 2:

- http://www.techworld.com/security/surviving-ransomware-kaspersky-lab-offers-advice-on-coping-with-extortion-attack-3626776/

Waste water treatment plant attack - slide 1:

- https://commons.wikimedia.org/wiki/File%3AWWTP_Antwerpen-Zuid.jpg

Waste water treatment plant attack - slide 2:

- https://commons.wikimedia.org/wiki/File%3AAS400.jpg
- By The original uploader was Ralbisser at German Wikipedia (Transferred from de.wikipedia to Commons.) [GFDL (http://www.gnu.org/copyleft/fdl.html) or CC-BY-SA-3.0 (http://creativecommons.org/licenses/by-sa/3.0/)], via Wikimedia Commons

Taking control of tram switch - slide 1:

- https://commons.wikimedia.org/wiki/File%3APESA_120Na-Warsaw001.jpg
- By Mateusz Włodarczyk (Own work) [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

Taking control of tram switch - slide 2:

- https://www.wired.com/2008/01/polish-teen-hac/

Disclosure of documents from a nuclear power plant - slide 1:

- https://commons.wikimedia.org/wiki/File%3ACANDU_at_Qinshan.jpg
- Atomic Energy of Canada Limited [Attribution], via Wikimedia Commons

Disclosure of documents from a nuclear power plant - slide 2:

- https://commons.wikimedia.org/wiki/File%3AAS04790183.jpg
- By IAEA Imagebank (Flickr: 04790183) [CC BY-SA 2.0 (http://creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons

Denial of service in car factories- Zotob - slide 1:

- https://commons.wikimedia.org/wiki/File%3AAS3.jpg
- By Brian Snelson (originally posted to Flickr as Final assembly) [CC BY 2.0 (http://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons

Denial of service in car factories- Zotob - slide 2:

- https://commons.wikimedia.org/wiki/File%3AHyundai_car_assembly_line.jpg
- By User: Anonyme (Own work) [GFDL (http://www.gnu.org/copyleft/fdl.html), CC-BY-SA-3.0 (http://creativecommons.org/licenses/by-sa/3.0/) or CC BY 2.5 (http://creativecommons.org/licenses/by/2.5)], via Wikimedia Commons

Discharge of waste water- slide 1:

- http://traitementdeseaux.fr/eaux-industrielles/

Discharge of waste water- slide 2:

- http://www.eham.net/classifieds/detail/335053

Explosion of a pipeline - slide 1:

- https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

Explosion of a pipeline - slide 2:

- https://commons.wikimedia.org/wiki/File%3ABaku_pipelines.svg
- By Thomas Blomberg (Own work) [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0) or GFDL (http://www.gnu.org/copyleft/fdl.html)], via Wikimedia Commons

Taking control of a motor vehicle - slide 1:

- https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

Taking control of a motor vehicle - slide 2:

- http://in.reuters.com/article/us-cybersecurity-autos-senators-idINKCN0RG2B420150916

Destruction of an information system – Shamoon – slide 1:

- http://www.gulfeyes.net/saudi-arabia/503401.html

Destruction of an information system – Shamoon – slide 2:

- https://www.theguardian.com/business/2011/jul/31/vedanta-resources-cairn-energy-india-deal

Diversion of a reconnaissance drone – slide 1:

- http://www.defensetech.org/2011/12/08/iranian-tv-shows-captured-rq-170/

Diversion of a reconnaissance drone – slide 2:

- https://commons.wikimedia.org/wiki/File%3ARQ-170_Wiki_contributor_3Dartist.png
- © TruthDowser / Wikimedia Commons, در ویکی‌انبار

Taking control of the manufacturing system of a steelworks - slide 1:

- http://www.france-metallurgie.com/portrait-de-lacierie-badische-stahlwerke/

Taking control of the manufacturing system of a steelworks - slide 2:

- http://www.bbc.com/news/technology-30575104

Disruption of rail signaling systems - Sobig/Blaster - slide 1:

- http://www.forbes.com/pictures/fjle45jhgk/the-top-50-military-friendly-employers/#17c8ea971daf

Disruption of rail signaling systems - Sobig/Blaster - slide 2:

- http://toastytech.com/guis/win98.html

Blackout in Ukraine - BlackEnergy - slide 1:

- https://industriemagazin.at/a/demand-response-wie-die-industrie-jetzt-ihren-energiebedarf-in-virtuellen-pools-optimiert?utm_source=Der+gro%C3%9Fe+Paketdienste-Test+in+der+Juni-Ausgabe+von+INDUSTRIEMAGAZIN&utm_medium=E-Mail-Newsletter&utm_content=HTML&utm_term=Artikel+(Titel)

Blackout in Ukraine - BlackEnergy - slide 2:

- https://www.washingtonpost.com/news/worldviews/wp/2015/11/21/saboteurs-blow-up-transmission-towers-knocking-out-power-to-crimea-russian-government-says/

Data exfiltration from energy companies- slide 1:

- http://www.alalam.ir/news/1648514

Data exfiltration from energy companies- slide 2:

- http://www.federaltimes.com/story/government/cybersecurity/2016/06/14/apt28-sofacy-us-officials/85866698/

Compromising of a computer network - slide 1:

- http://www.huffingtonpost.ca/2012/09/28/calgary-telvent-security--hacking-chinese_n_1924078.html

Compromising of a computer network - slide 2:

- http://www.industrytap.com/world-pre-911-moment-digital-war-heats/24624

Explosion of a gas pipeline - slide 1:

- http://www.euractiv.com/section/europe-s-east/news/ukraine-suspects-russian-foul-play-behind-pipeline-blast/

Explosion of a gas pipeline - slide 2:

- https://southfront.org/main-gas-pipeline-stavropol-moscow-was-blown-up-near-the-city-rovenki/

Poisoning of drinking water – slide 1:

- http://kitprofs.com/services/water/

Poisoning of drinking water – slide 2:

- https://www.compricer.se/nyheter/artikel/sparpengar-ar-skyddade-av-insattningsgarantin--men-hur-ar-det-med-fonder-och-aktier

Emergency shutdown of a nuclear reactor – slide 1:

- http://www.ledauphine.com/actualite/2011/03/14/un-(petit)-reacteur-nucleaire-a-grenoble

Emergency shutdown of a nuclear reactor – slide 2:

- http://courrierstrategique.com/4899-russie-construction-des-reacteurs-nucleaires-en-iran.html

Attack on an insulin pump – slide 1:

- http://discovermagazine.com/2016/may/13-priming-the-pump

Attack on an insulin pump – slide 2:

- http://www.startribune.com/supreme-court-won-t-block-medtronic-liability-case/264836081/

Icon credits:

- http://flaticon.com