Club de la sécurité de l'information français

CLUSIF

Fiches Incidents Cyber SI Industriels

CLUSIF – Groupe de Travail SCADA

Avril 2017

Club de la sécurité de l'information français

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement:

Les responsables du groupe de travail:

Anthony	DI PRIMA	*Wavestone*
Hervé	SCHAUER	*HSC by Deloitte*

Les contributeurs:

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	*Ministère de la Défense*	Jérôme	RICHARD	*Econocom Digital Security*
Pascal	SITBON	*Seclab*	Ilias	SIDQUI	*Wavestone*

Le CLUSIF remercie également les adhérents ayant participé à la relecture.

Pour tout commentaire, veuillez contacter le CLUSIF à l'adresse suivante : scada@clusif.fr

Sommaire

Présentation du Groupe de Travail "Sécurité SCADA"

GT SCADA

- Le Groupe de Travail SCADA est un groupe d'échange et de partage entre les acteurs de la sécurité informatique du monde industriel. Il regroupe notamment des RSSI, des architectes, des éditeurs et des consultants.
- Les objectifs du groupe sont d'échanger sur les pratiques en matière de cybersécurité des systèmes industriels, d'analyser les tendances actuelles et les évolutions réglementaires.
- Le groupe, créé en 2013, a mené plusieurs travaux qui ont abouti entre autres à la publication d'un panorama des référentiels de sécurité[1].
- En 2016, le GT s'est penché sur les enseignements à tirer des cas d'incidents et d'attaques survenus sur des systèmes industriels avec des conséquences plus ou moins graves selon les cas.

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

Présentation du document

Objectifs

- Les fiches présentées dans ce document ont pour objectif de sensibiliser à la cybersécurité en environnement industriel à partir de cas réels d'attaques, d'incidents ou de preuves de concept pour leur dimension didactique.

- Outre les responsables sécurité des systèmes d'information, le document s'adresse à une population plus large, telle que des techniciens, mainteneurs, intégrateurs, éditeurs, responsables informatiques, responsables d'exploitation et industriels voire des directions générales, amenés à traiter cette problématique.

Démarche adoptée

1 Identification

Dans un premier temps il a été décidé d'**énumérer** l'ensemble des incidents connus des membres du GT.

L'ensemble de recherche était ouvert à **tous les secteurs d'activité**, **tous les pays**. Aucune restriction temporelle n'a d'ailleurs été fixée.

Les contributeurs ont identifié une multitude d'attaques et incidents cyber.

L'apport a été réalisé à partir de **sources ouvertes, publiques**.

2 Sélection

Les incidents selectionnés ayant fait l'objet d'une fiche devaient répondre aux critères suivants:

- **Suffisamment d'éléments** disponibles pour décrire les incidents, le déroulé de l'attaque et les impacts;
- **Sources multiples, concordantes et vérifiables** (magazines, sites web d'information, rapports émanant d'organismes);
- **Atteinte du SI industriel** ou **de son environnement proche**, **ou impact sur la production ou l'exploitation industrielle**.

3 Restitution

Les membres du GT se sont répartis la rédaction des fiches incidents.

Chaque fiche est constituée de 2 pages:

- **Un visuel** et une **description synthétique de l'attaque**;
- Le **déroulé et les impacts** basés sur les sources préalablement identifiées ainsi que les **recommandations du Clusif**.

Comment lire les fiches? 1/2

Présentation du contexte de l'attaque:
- Année(s) au cours de laquelle s'est déroulée l'attaque;
- Secteur d'activité de l'entité touchée;
- Lieu où se trouve l'entité touchée par l'attaque.

Titre de la fiche

Description succincte du scénario d'attaque ou de l'incident et son impact

Visuel illustratif de l'incident

Vulnérabilité exploitée pour mener l'attaque

Comment lire les fiches? 2/2

La gravité de l'attaque dépend des impacts constatés. 4 niveaux de gravité ont été identifiés:

- Faible: pas ou peu d'impact
- Moyenne : perte de production ponctuelle, pas d'impact humains, pas d'impacts écologique
- Élevée : perte de production lourde, blessés mais pas de décès, impact écologique
- Majeure : impacts financiers et/ou humains très lourds

Une description du déroulé de l'attaque basée sur les informations recueillies et consolidées par les contributeurs du GT.

Prise de contrôle d'un véhicule automobile

CLUSIF

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

La complexité de l'attaque dépend des moyens mis en œuvre. 4 niveaux de complexité ont été identifiés:

- Faible : pas d'outil nécessaire
- Moyenne : outillage nécessaire, compétence technique simple à acquérir par l'attaquant
- Élevée : outillage nécessaire, compétence technique forte et spécifique
- Très Elevée: développement spécialisé pour l'attaque avec des moyens financiers et humains très importants

Les conclusions à tirer de cette attaque ainsi que les messages à transmettre sont présents dans cet encadré.

Rappel du contexte

Quelque(s) source(s) utilisée(s) pour l'élaboration de la fiche

Incidents analysés

Énergie

Fiche 1	Interruption de production d'électricité	France	2015
Fiche 2	Coupure générale d'électricité - BlackEnergy	Ukraine	2015
Fiche 3	Exfiltration de données de compagnies d'énergie - Havex	Europe/USA	2013-2014
Fiche 4	Compromission du réseau informatique	Canada	2012

Pétrole & Gaz

Fiche 5	Explosion d'un pipeline	Turquie	2008
Fiche 6	Destruction d'un système d'information - Shamoon	Arabie saoudite	2012
Fiche 7	Explosion d'un gazoduc	URSS	1982

Incidents analysés

Eau/assainissement

Fiche 8	Attaque d'une station d'épuration des eaux	N/C	2015
Fiche 9	Mise hors service d'un superviseur de dérivation d'eau	USA	2007
Fiche 10	Déversement d'eaux usées	Australie	2000
Fiche 11	Empoisonnement de l'eau potable	USA	2013

Transport

Fiche 12	Prise de contrôle de l'aiguillage d'un tramway	Pologne	2008
Fiche 13	Prise de contrôle d'un véhicule automobile	USA	2015
Fiche 14	Perturbation des systèmes de signalisation ferroviaire – Sobig/Blaster	USA	2003

Incidents analysés

Industrie

Fiche 15	Déni de service sur usines automobiles - Zotob	USA	2005
Fiche 16	Prise de contrôle du système de production d'une aciérie	Allemagne	2014

Nucléaire

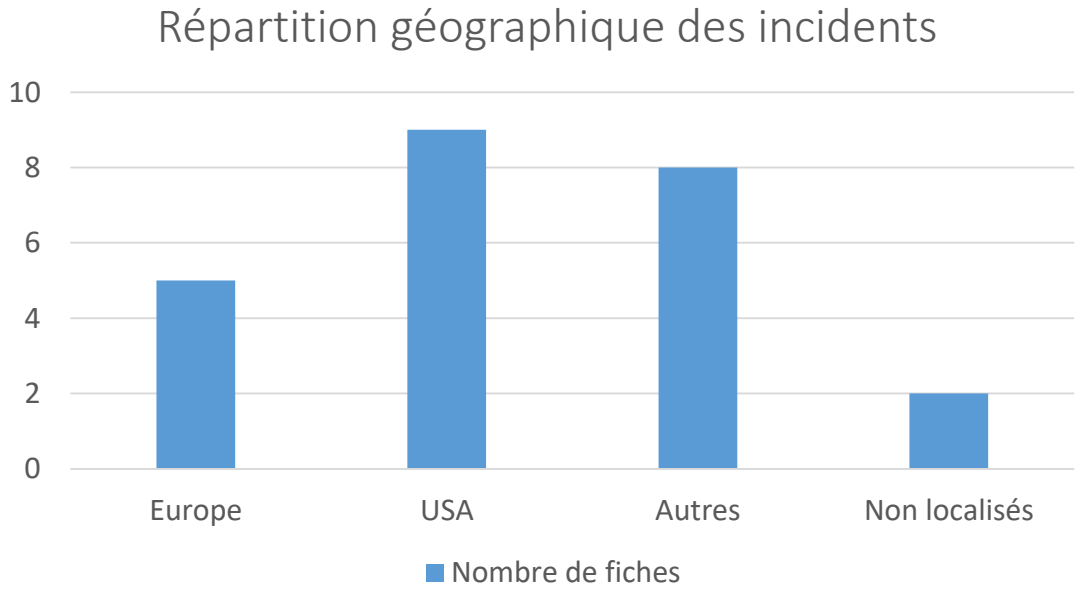
Fiche 17	Divulgation de documents d'une centrale nucléaire	Corée du Sud	2014
Fiche 18	Sabotage d'un processus industriel - Stuxnet	Iran	2009-2010
Fiche 19	Infection par ver dans une centrale nucléaire - Slammer	USA	2003
Fiche 20	Arrêt d'urgence d'un réacteur nucléaire	USA	2008

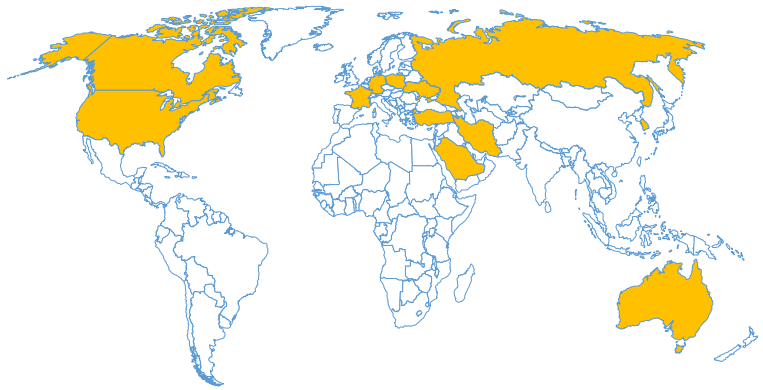
Autre

Fiche 21	Détournement d'un drone de reconnaissance	Iran	2011
Fiche 22	Attaque de terminaux de points de vente - BlackPOS	USA	2013
Fiche 23	Attaque sur une pompe à insuline	Monde	2011

Analyse des incidents

- L'analyse de la répartition géographique des incidents dévoile plusieurs éléments sur la situation économique et réglementaire des pays. En effet on remarque que :
  - Les pays les plus touchés sont les pays industrialisés disposant d'une industrie automatisée.
  - Le pays le plus représenté par ces fiches est les USA. Ceci pourrait s'expliquer par la culture de transparence sur ces sujets, avec de plus une réglementation obligeant les entreprises à signaler certains incidents.

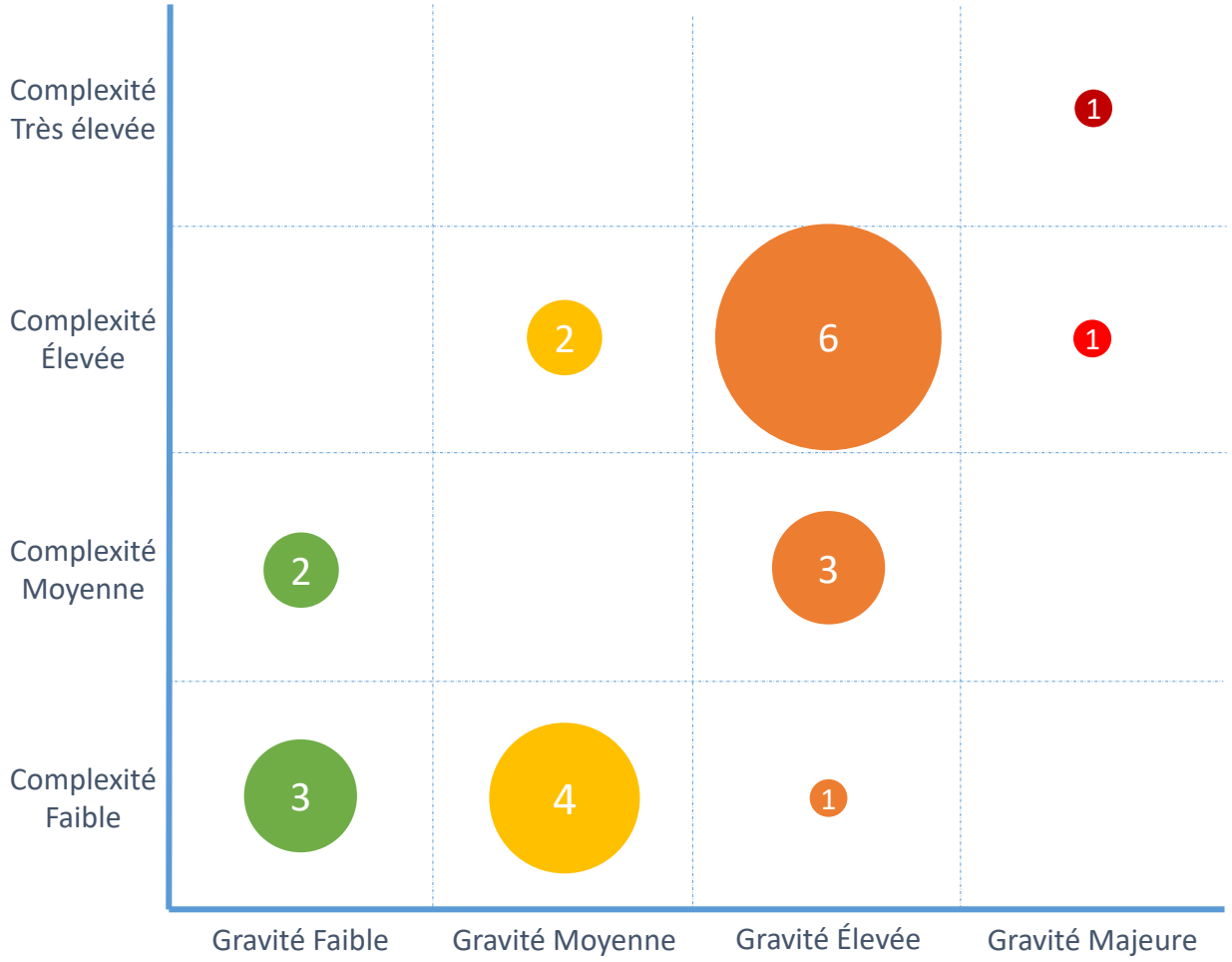




Analyse des incidents

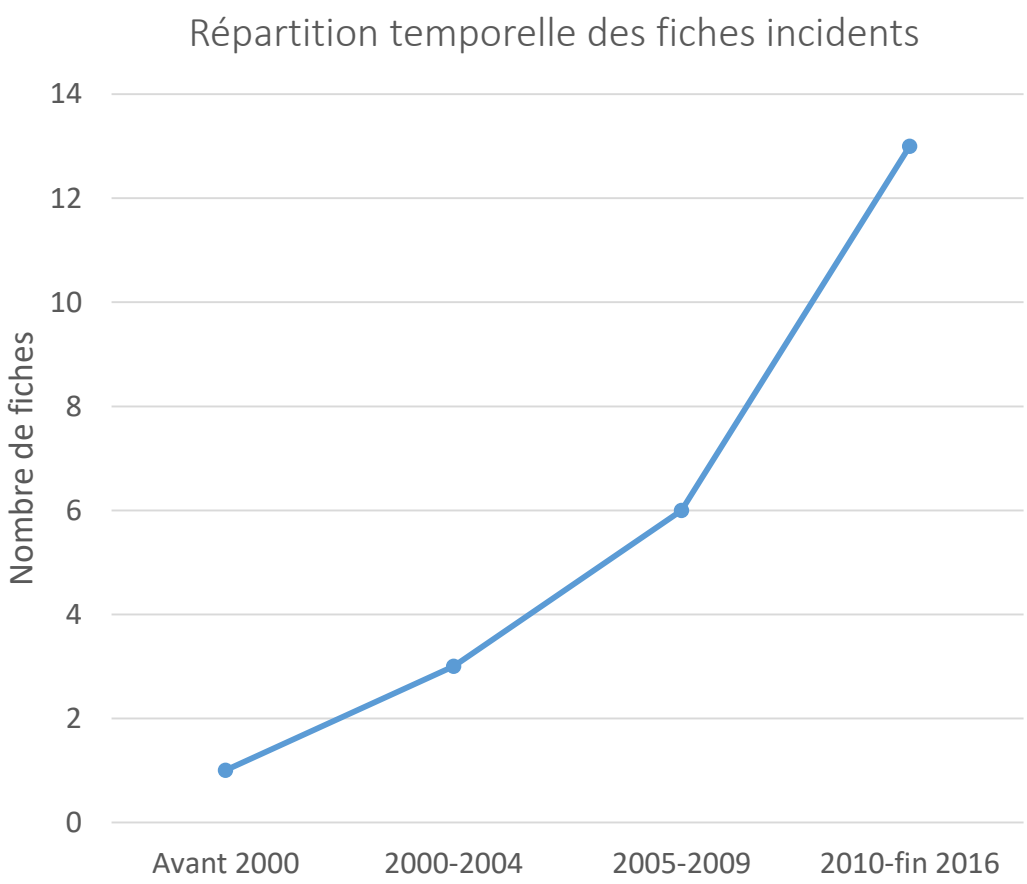
- Le GT SCADA a référencé des attaques sur systèmes industriels dont se sont fait écho la presse et les organismes de sécurité, et cela **quelle que soit leur gravité**.
- Les fiches ont été réparties selon **4 degrés de gravité** (faible, moyenne, élevée et majeure). Pour chaque incident, la complexité de l'attaque a été évaluée selon **les informations disponibles et publiques**. L'évaluation de la complexité s'est faite sur **4 niveaux** (faible, moyenne, élevée et très élevée).
- L'étude croisée de la gravité et complexité des attaques ou incidents permet d'en tirer quelques enseignements :
  - Les attaques de gravité majeure ont un niveau de complexité élevé voire très élevé: elles sont rendues possibles si l'attaquant dispose de **moyens financiers et matériels conséquents** et un **haut niveau d'expertise**. En effet, une attaque sur un système industriel nécessite une connaissance pointue du métier et des processus associés.
  - Cette connaissance ne peut être atteinte que lorsque d'importants moyens ont été mis en place pour la conception de l'attaque, par exemple dans le cas de l'attaque sur le système de distribution d'électricité en Ukraine. Ceci peut expliquer en partie pourquoi **de telles attaques sont encore peu nombreuses**.
  - Le graphique montre que **plusieurs attaques de faible complexité** ont pu avoir des **impacts de gravité moyenne voire élevée**. Ceci illustre bien que **les bonnes pratiques en matière de sécurité ne sont pas toujours appliquées sur les systèmes**.

Nombre de fiches par gravité/incidents



Analyse des incidents

- Les incidents présentés dans ce document représentent une partie des attaques sur les systèmes industriels relayées par la presse ou par les organismes de sécurité.
- Il est à noter que dans le périmètre de ce travail, les attaques ayant eu un impact sur les systèmes de production ou les systèmes d'information industriels (ou réseau proche) sont en **constante augmentation**. Plusieurs facteurs peuvent expliquer cette tendance qui se confirme d'année en année, mais la plus importante est **la connectivité numérique accrue des systèmes industriels**.
- En effet, l'**ouverture** des systèmes industriels aux technologies qui étaient propres au domaine de la bureautique a rendu ces systèmes **vulnérables aux attaques informatiques**.
- De plus, il transparaît au travers de l'analyse de ces différentes attaques que cette transformation des systèmes industriels n'a pas été accompagnée par des **mesures de sécurité adéquates**. **Toutes les mesures possibles sont détaillées par des référentiels de sécurité dont le CLUSIF a dressé un panorama en 2014**. Ce panorama fait actuellement l'objet d'une mise à jour par les membres du GT SCADA, dont la publication est prévue en 2017.



Synthèse

Les incidents sont en nombre croissant, avec plusieurs causes :

- La généralisation des standards des technologies de l'information (IT) : la plupart des protocoles industriels sont à présent déclinés sur TCP/IP, et de plus en plus de logiciels de niveau 2 (supervision, historisation…) voire des composants de niveau 1 (PLC, RTU…) fonctionnent sur des systèmes d'exploitation issus du monde IT.
- L'interconnexion des réseaux industriels avec les réseaux de bureautique, dans des objectifs de performance, de reporting et d'économie.
- Plus généralement, l'ouverture à des systèmes tiers : la sous-traitance des projets, les astreintes distantes et l'externalisation de la maintenance multiplient les accès aux réseaux industriels.

Les principales mesures qui auraient été efficaces au vu de cette liste d'incidents sont :

- Le contrôle des flux logiques (réseaux) et physiques (circulation des personnes, clés USB, PC portables…) aux interconnexions entre le SI de gestion et le SI industriel, et au sein du SI industriel.
- La maîtrise des accès externes aux systèmes industriels avec authentification forte, validation locale, procédure d'isolement en cas d'alerte.
- La surveillance des flux afin de détecter des attaques: les intrusions les plus complexes étant précédées de phases de reconnaissance, la maitrise par l'exploitant des flux légitimes sur son réseau industriel doit permettre de repérer les activités anormales.

Quelles tendances pour les années à venir?

- L'évolution croissante, mais modérée, des incidents reflète en partie **l'augmentation du niveau de menace et de la vulnérabilité** des SI industriels
- La « **démocratisation** » des logiciels d'attaque, comme par exemple la publication du code source Mirai[1], permet à des acteurs avec des moyens limités de réutiliser ces outils à moindre frais : à chaque attaque étatique (Stuxnet, Shamoon, Ukraine) il y a transfert d'idées voire d'outils. Avec **l'émergence de l'industrie 4.0**, l'introduction massive des objets connectés au niveau terrain risque **d'étendre considérablement le niveau d'exposition des SI industriels.** Leur utilisation en contexte urbain introduit aussi des problématiques liées à **la protection des données à caractère personnel** (jusqu'à présent restreintes aux SI de gestion).
- Les **réglementations** se renforcent et exigent dorénavant un niveau minimum de cybersécurité pour les infrastructures critiques qui pour la plupart d'entre elles sont constituées de systèmes industriels.
- Les états se dotent d'un **arsenal cyber** afin d'être en mesure de mener des opérations sur le théâtre cyber : **les systèmes industriels étant des cibles de premier choix** pour la déstabilisation d'un état au regard des impacts que peuvent engendrer les attaques.

Dans ce contexte l'enjeu est de savoir si la prise de conscience du niveau de risque et les plans de sécurisation vont se faire assez rapidement et être suffisamment ambitieux avant que des incidents graves ne surviennent.
Le CLUSIF espère y contribuer via ce jeu de « fiches incidents ».

[1] https://fr.wikipedia.org/wiki/Mirai_(logiciel_malveillant)

Fiches incidents

Interruption de production d'électricité

Impact

Arrêt de production d'électricité pendant **15 jours**

Scénario d'incident

Impossibilité d'accéder au système de communication avec l'hydrolienne à cause d'un **rançongiciel**

Vulnérabilité

Connectivité directe à Internet du système sans protection (absence de pare-feu)

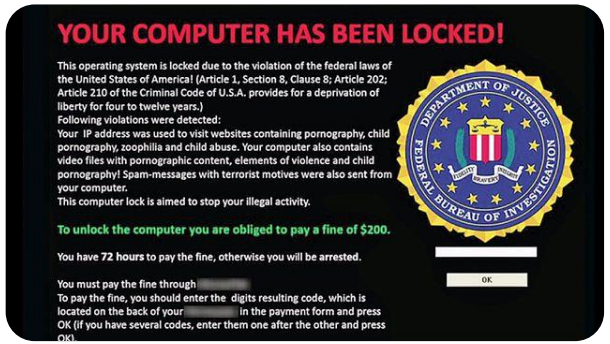
Interruption de production d'électricité

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Faible	Financière	Faible

Déroulement de l'attaque

- Les attaquants ont **chiffré le serveur** permettant la connexion satellitaire avec l'unité de pilotage de l'hydrolienne.
- Ils ont demandé **une rançon de 4000$** à payer par PayPal ou par bitcoin afin de rétablir la connexion.
- Sabella a refusé de payer ce qui a conduit à **une interruption du système** en phase de test pendant 15 jours.



Moyens mis en œuvre

- Un rançongiciel
- Connexion internet

Enseignement à tirer, préconisation et contre-mesures

- **Améliorer le contrôle** et la protection des **systèmes d'accès à distance** (authentification forte).
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Sécurité périmétrique** : Installation d'un pare-feu, passerelle de rebond
  - Mise en place d'un **système redondant** afin d'assurer la continuité de la production
- **Maîtriser la communication de crise** :
  - Éviter de commenter les investigations en cours au risque de donner des informations erronées (attribution de l'attaque à des hackers russo-cubains) risquant d'impacter l'image de l'entreprise (Sabella était en cours de négociation pour développer de nouveaux marchés internationaux)
  - Ne pas dévoiler les nouveaux moyens de protection mis en œuvre

2015 | Énergie | Ouessant, France | Ouest France, Usine Nouvelle

Coupure générale d'électricité - BlackEnergy

Impact

80 000 foyers ukrainiens privés d'électricité, interruption de 3 à 6h

Scénario d'incident

Déconnexion des postes électriques du réseau par un malware

Vulnérabilité

Naïveté des utilisateurs, manque de cloisonnement et de maîtrise des habilitations

Coupure générale d'électricité - BlackEnergy

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Stratégique inter-états	Élevée

Déroulement de l'attaque

- Une vague de «phishing » cible 3 compagnies de distribution d'électricité. Le mail comportait un fichier Word infecté qui, après ouverture et activation des macros installe le malware **BlackEnergy** sur le poste.
- Pour contourner le pare-feu séparant le SI industriel du SI de gestion, les attaquants **piratent l'active directory** (annuaire) et prennent le contrôle de comptes VPN permettant de commander à distance le SCADA.
- Les attaquants **reprogramment les onduleurs** et corrompent le firmware des passerelles « série vers Ethernet » des postes électriques afin de perturber les opérations de remédiation.
- Enfin, ils lancent l'attaque en **désactivant les onduleurs et les sous stations électriques**. Ils ont aussi lancé un déni de service téléphonique sur le call-center pour empêcher les usagers de déclarer les pannes.

Moyens mis en œuvre

- Un groupe d'individus expérimentés ayant une bonne connaissance des systèmes industriels et très fortes compétences techniques
- Malware (BlackEnergy)

Enseignement à tirer, préconisation et contre-mesures

- Les utilisateurs du SI doivent être sensibilisés au risque que représente le « spear phishing » (campagne de mails infectés). La formalisation de **plan de continuité d'activité** permet de réduire l'impact (2 mois après l'attaque, les compagnies de distribution touchées n'avaient toujours pas retrouvé de fonctionnement normal).
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Cloisonnement** plus important des réseaux (utilisation de diode par exemple)
  - **Blocage des macros Office**
  - **Sensibilisation** des employés à la sécurité
  - **Contrôle des habilitations** des utilisateurs (contrôle des droits d'écriture et modification des firmware)

2015 | Énergie | Ukraine | Sillicon.fr, SANS

Exfiltration de données de compagnies d'énergie - Havex

Impact

Vol de données

Scénario d'incident

Pénétration des réseaux internes des compagnies d'énergie grâce à des **malwares insérés dans des mises à jour logicielles de trois fournisseurs de systèmes industriels SCADA**

Vulnérabilité

Naïveté des utilisateurs, manque de test des mises à jour logicielles

Exfiltration de données de compagnies d'énergie - Havex

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Moyenne	Espionnage	Élevée

Déroulement de l'attaque

- Un groupe de hackers nommé Dragonfly a utilisé 3 stratégies différentes pour infecter les réseaux informatiques de plus de 1000 entreprises du secteur de l'énergie:
  - Envoi de mails contenant un **PDF infecté** à de hauts responsables d'entreprises du secteur de l'énergie.
  - Compromission de sites web en lien avec le secteur de l'énergie ayant pour effet une redirection vers des sites malfaisant **chargé d'infecter les visiteurs par des chevaux de Troie**.
  - Infection **des mises à jour de logiciels SCADA de 3 fournisseurs** en téléchargement libre sur leurs sites web. Les systèmes de contrôle commande dès lors qu'ils étaient mis à jour disposaient ainsi des portes dérobées utilisables par le groupe de hackers.

Moyens mis en œuvre

- Cheval de Troie (Karagany)
- Porte dérobée/Backdoor (Oldrea, Havex ou Energetic Bear RAT)
- Un groupe de personnes avec de très bonnes compétences techniques (nommé Dragonfly ou Energetic Bear)

Enseignement à tirer, préconisation et contre-mesures

- Les utilisateurs du SI doivent être sensibilisés au risque que représente le **« phishing »** (envoi de mails infectés). Les mises à jour des logiciels, même lorsqu'elles proviennent des éditeurs de solutions, peuvent être corrompues.
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Sensibilisation** des employés à la sécurité
  - Installation de **solutions de détection des changements de configuratio**n des ordinateurs (« whitelisting ») qui pourront détecter l'installation de portes dérobées
  - **Mise en place d'un processus de test des mises à jour des logiciels**

2013-2014	Énergie	Europe, USA	Rapport Symantec, BBC

Compromission du réseau informatique

Impact

Déconnexion des accès distants clients

Scénario d'incident

Vols de données clients (mot de passe accès distant NOC) et vol d'informations concernant leur produit OASyS SCADA

Vulnérabilité

Contournement des pare feu

Compromission du réseau informatique

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Moyenne	Espionnage	Élevée

Déroulement de l'attaque

- Telvent est une entreprise qui conçoit des logiciels SCADA.
- Le groupe de hackers chinois a pu infecter le réseau de Telvent en contournant un **pare feu interne**.
- Les attaquants ciblaient le logiciel OASyS SCADA et avaient pour but de modifier les fichiers clients.
- Les attaquants ont réussi à avoir accès au SI de gestion de Telvent.
- S'ils avaient pu mener leur attaque jusqu'au bout, ils auraient pu modifier le code du logiciel SCADA.
- Après avoir remarqué l'attaque, **Telvent a informé ses clients et a coupé toutes les connexions avec eux.**

Moyens mis en œuvre

- Groupe de hackers chinois portant le nom de *Comment Group*

Enseignement à tirer, préconisation et contre-mesures

- Les entreprises développant des logiciels pour SI Industriel doivent **protéger les environnements de développement** et s'assurer qu'il sont **cloisonnés du reste du SI**.
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Sensibilisation des employés à la sécurité**
  - **Cloisonnement des environnements de développement**

- Point positif : Alors qu'elle n'était pas légalement obligée de le faire, **Telvent a informé ses clients de l'attaque**.

Explosion d'un pipeline

2008 | Pétrole & Gaz | Turquie | Fiche 5

Origine informatique de l'incident contestée

Impact

Destruction du pipeline de Baku-Tbilisi-Ceyhan (BTC), Destruction de matériel, 20 jours d'indisponibilité (plus de **1 Md$** de pertes en matériel et recettes)

Scénario d'incident

Désactivation des systèmes de monitoring et **d'alarmes** puis explosion

Vulnérabilité

Logiciel des caméras, accès aux vannes, réseau radio exposé

Explosion d'un pipeline

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Stratégique inter-états	Élevée

Déroulement de l'attaque

- Les caméras de surveillance installées le long du pipeline étaient vulnérables et connectées au centre de surveillance via Internet. En exploitant ces vulnérabilités, des attaquants ont pu accéder au serveur de gestion des alarmes (lui aussi vulnérable) présent dans le centre. Ils ont désactivé les alarmes de sûreté et les moyens de communication des équipes locales (en brouillant la communication sans fil).
- En se rendant à une station de pompage, les attaquants manipulèrent les systèmes industriels (postes industriels ou automates) provoquant une montée de pression dans le pipeline et son explosion.
- Le centre de surveillance du pipeline a eu connaissance de l'explosion 40 minutes après qu'elle ait eu lieu grâce au signalement réalisé par un technicien présent sur les lieux au moment de l'incident.

Moyens mis en œuvre

- Attaque combinée physique et cyber
- Désactivation des caméras de surveillance et des alarmes
- Manipulation des systèmes industriels

Enseignement à tirer, préconisation et contre-mesures

- **La vérification de la disponibilité des moyens de surveillance** est nécessaire pour assurer la sécurité cyber du SI industriel. L'absence de réponse d'un système d'alarme est un incident en soi. De plus, la **sécurité des accès physiques** est un paramètre primordial dans la sécurité des SI industriels.
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Diversification des moyens de surveillance**
  - **Durcissement des systèmes industriels** et des **contrôles d'accès physiques**
  - **Cloisonnement des systèmes**
  - **Maintien en condition de sécurité des équipements** (ex: caméras et serveur vulnérables)

Destruction d'un système d'information - Shamoon

2012 | Pétrole & Gaz | Dhahran, Arabie Saoudite | Fiche 6

Impact

Incapacité à livrer les clients, **facturation partielle**, **retour à la normale après 5 mois**

Scénario d'incident

Destruction totale ou partielle et suppression de fichiers sur **30 000 postes de travail et 2 000 serveurs**

Vulnérabilité

Manque de sensibilisation des collaborateurs

Destruction d'un système d'information - Shamoon

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Politiques	Moyenne

Déroulement de l'attaque

- Un employé de la compagnie ayant un compte privilégié a probablement cliqué sur un lien contenu dans un message SCAM (**hameçonnage**).
- Le **virus Shamoon** s'est rapidement déployé à l'ensemble du réseau **30000 postes de travail, 2000 serveurs.**
- Le virus exfiltrait les fichiers des postes et serveurs, puis les supprimait. Ensuite, le virus détruisait les machines **en réécrivant le secteur d'amorçage** du disque.
- Le cœur de métier a été impacté: gestion des commandes, des stocks, livraison, facturation… Seule l'extraction pétrolière n'a pas été affectée (officiellement, réseau SCADA séparé).

Moyens mis en œuvre

- Virus Shamoon
- Investissement financier faible
- Aucun matériel spécifique

Enseignement à tirer, préconisation et contre-mesures

- La **sensibilisation** des utilisateurs reste un point important à prendre en compte.
- Les réseaux à plat permettent aux malware de se déployer très facilement.
- Les mesures suivantes auraient permis de s'en prémunir ou d'en limiter la portée:
  - Mettre en place des **système de détection d'intrusion**
  - Segmenter le réseau par niveau de sensibilité
  - **Sensibiliser** les employés à la sécurité
  - Mettre en place **un plan de continuité d'activité** en spécifiant l'utilisation de matériel de rechange

2012 | Pétrole & Gaz | Arabie Saoudite | CNN, NY times

Explosion d'un gazoduc

Origine de l'incident contestée

Impact

Explosion du gazoduc Urengoy–Pomary–Uzhgorod, pas de victime

Scénario d'incident

Surpression dans le gazoduc causée par un cheval de Troie et une bombe logique

Vulnérabilité

Logiciel piégé volé par le KGB à une firme Canadienne

Explosion d'un gazoduc

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Stratégique inter-états	Élevée

Déroulement de l'attaque

- Grâce aux documents divulgués par un agent double de la CIA infiltré dans les rangs du KGB (« Dossiers Farewell »), la CIA était au courant des vols de technologies massifs par l'URSS (Line X).
- La CIA aurait alors piégé ses technologies (dont des logiciels) afin de riposter contre l'URSS et discréditer les technologies déjà volées.

Moyens mis en œuvre

- Stratégie étatique
- Confidentialité forte
- Modification du code des logiciels

Enseignement à tirer, préconisation et contre-mesures

- Un logiciel ou une technologie peut **contenir des chevaux de Troie**, **des portes dérobées**, etc…
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Audit du code source des logiciels**
  - **Installation de mécanismes de sécurité indépendants du système informatique** (ex: systèmes de sûreté)

2012 | Pétrole & Gaz | URSS

At he Abyss : An insider'sHistory of the Cold war (ISBN 0-89141-821-0)

Attaque d'une station d'épuration des eaux

Impact

Perturbation du procédé de traitement de l'eau

Scénario d'incident

Modification des dosages des produits chimiques utilisés pour le traitement de l'eau

Vulnérabilité

Faille dans une application en ligne reliée au système industriel

Attaque d'une station d'épuration des eaux

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Faible	Fraude	Faible

Déroulement de l'attaque

- L'attaquant a pris **le contrôle de l'application de paiement en ligne** afin de voler des données clients.
- Le serveur exécutant cette application (un AS400) hébergeait **les données de connexion d'un compte administrateur** ainsi **que l'adresse IP du serveur** gérant le processus industriel. En utilisant ces données l'attaquant a eu **accès à l'interface de contrôle de l'installation**.
- L'attaquant a modifié les paramètres de l'application entraînant une perturbation dans le procédé de traitement des eaux.
- Les perturbations ont été limitées grâce à la réactivité des équipes industrielles qui ont rétabli un fonctionnement correct du processus industriel grâce à **leurs échanges** avec les équipes IT.

Moyens mis en œuvre

- Outils de hacking basiques (injection SQL)
- Très peu de connaissance des systèmes SCADA
- Aucune connaissance particulière sur le fonctionnement du processus industriel

Enseignement à tirer, préconisation et contre-mesures

- **L'absence de contrôle entre le système industriel et le système de paiement en ligne**, le **faible niveau d'authentification** et la **mauvaise protection des mots de passe** rendent le système industriel vulnérable aux attaques provenant d'Internet.
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Ségrégation** entre le système d'information industriel et celui de gestion
  - Implémentation d'une **authentification forte** pour l'accès aux systèmes industriels
  - Réalisation d'**audits récurrents** des applications exposées sur Internet pour identifier les vulnérabilités connues
- Point Positif : **Système de sûreté**, é**changes** entre les équipes IT et industrielles suite à un comportement suspect.

2015	Eau / Assainissement	Lieu non communiqué	Verizon report, The register

Mise hors service d'un superviseur de dérivation d'eau

Impact

Déni de service du superviseur / **5000 $ de dommages**

Scénario d'incident

Employé licencié a endommagé le superviseur

Vulnérabilité

Manque de suivi des droits d'accès des employés

Mise hors service d'un superviseur de dérivation d'eau

Club de la sécurité de l'information français

CLUSIF

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Faible	Vengeance	Faible

Déroulement de l'attaque

- Un **ancien employé** du Tehama Colusa Canal Authority a intentionnellement installé **un logiciel non autorisé** sur l'ordinateur chargé de dériver l'eau de la rivière Sacramento à des fins d'irrigation.
- L'installation de ce logiciel **a endommagé l'ordinateur** faisant partie du SCADA.
- Les opérateurs ont alors basculé en pilotage manuel.

Moyens mis en œuvre

- Une seule personne avec des connaissances faibles
- Investissement financier faible
- Un accès libre au superviseur

Enseignement à tirer, préconisation et contre-mesures

- Il est important de ne pas négliger les **menaces provenant de l'intérieur** de l'entreprise (salarié mécontent, erreurs de manipulation …).
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Limitation des droits des utilisateurs**
  - **Procédure de révocation des droits des collaborateurs** (départ, changement d'affectation, mutation)
  - **Surveillance** du changement de la configuration du superviseur
- Point positif: Les opérateurs avaient toujours la possibilité de basculer en **pilotage manuel** limitant les dommages causés par cet incident.

2007 | Eau / Assainissement | Willows, USA | Computer world

Déversement d'eaux usées

Impact

800 m³ d'eaux usées déversées dans des rivières et parcs

Scénario d'incident

Prise de contrôle à distance par un candidat éconduit

Vulnérabilité

Réseau radio d'accès distant sans authentification

Déversement d'eaux usées

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Vengeance	Faible

Déroulement de l'attaque

- Un **ex-employé** de la société ayant installé le système SCADA de la centrale de traitement des eaux usées de la Maroochy Shire a postulé pour un poste au sein de cette dernière.
- Sa demande d'emploi ayant été refusée, il a décidé de **se venger** des 2 employeurs en prenant le contrôle de la station. Il a donc **volé un équipement radio de son employeur** et a envoyé des commandes au système de contrôle qu'il a aidé à installer.
- Les commandes envoyées lui ont permis de déverser des centaines de milliers de litres d'eaux usées.
- **Sa connaissance du processus industriel** lui a permis de faire croire que ses actions étaient dues à un dysfonctionnement du système.

Moyens mis en œuvre

- Une seule personne avec des connaissances techniques et du processus industriel
- Investissement financier faible
- Un équipement radio volé

Enseignement à tirer, préconisation et contre-mesures

- **La supervision des équipements** ainsi que des droits d'accès est une partie intégrante de la sécurité.
- L'utilisation d'un protocole véhiculé en clair même s'il est propriétaire ne protège pas contre des attaques.
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Mécanismes anti-rejeu** pour éviter des attaques simples visant à rejouer des ordres ou opérations légitimes
  - **Supervision** pour remonter le fil des événements et procédures de gestion d'incidents
  - Mise en place d'un processus de **contrôle des habilitations et des équipements**
  - **Sensibilisation des collaborateurs** pour distinguer les dysfonctionnements des cas d'attaques réelles.

2000	Eau / Assainissement	Maroochy, Australie	The Register, Rapport NIST

Empoisonnement de l'eau potable

Impact

400 résidents privés d'eau

Scénario d'incident

Modification réglages des taux de fluor et de chlore

Vulnérabilité

Manque de surveillance de l'installation. Accès physique possible sans levée d'alerte

Empoisonnement de l'eau potable

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Moyenne	Vengeance?	Faible

Déroulement de l'attaque

- Les attaquants se sont introduits dans la station **en passant au-dessus des barbelés**.
- Aucune effraction aux portes et aux fenêtres.
- Les attaquants ont eu accès au **système de supervision** et ont **modifié les réglages** des taux de fluor et de chlore.
- Les véhicules des employés possèdent des GPS et attestent qu'aucun d'entre eux n'était près de la station durant l'incident.
- La société gestionnaire de la station a informé la population de l'attaque.

Moyens mis en œuvre

- Une ou plusieurs personnes avec une connaissance de la station
- Pas d'investissement financier

Enseignement à tirer, préconisation et contre-mesures

- La **sécurité des accès physiques** est un paramètre à prendre en compte lors de la sécurisation des SI industriels.
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Contrôle d'accès physique** renforcé
  - **Surveillance des zones à risques**
  - **Révocation des accès au départ d'un employé**
  - **Supervision de la sécurité**

Prise de contrôle de l'aiguillage d'un tramway

Impact

4 tramways déraillés, 12 blessés légers

Scénario d'incident

Prise de contrôle du système d'aiguillage par un adolescent

Vulnérabilité

Réseau radio sans authentification

Prise de contrôle de l'aiguillage d'un tramway

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Ludique / Par challenge	Moyenne

Déroulement de l'attaque

- Dans la ville de Lodz en Pologne, un adolescent s'est infiltré dans le dépôt des tramways de la ville et **a étudié le réseau** ainsi que les tramways pendant **une longue période**.
- Il a alors modifié une **télécommande de télévision** afin de lui permettre de modifier les aiguillages du réseau de tramway.
- Sans avoir conscience de ses actes, l'adolescent a fait dérailler 4 tramways en modifiant l'aiguillage blessant 12 personnes.

Moyens mis en œuvre

- Une seule personne avec des connaissances de niveau académique
- Investissement financier faible
- Une télécommande de TV modifiée

Enseignement à tirer, préconisation et contre-mesures

- L'utilisation d'un protocole véhiculé **en clair** même s'il est propriétaire ne protège pas contre des attaques.
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Authentification mutuelle** pour s'assurer que seuls les équipements autorisés peuvent communiquer avec le système d'aiguillage
  - **Mécanismes anti-rejeu** pour éviter des attaques simples visant à rejouer des ordres ou opérations légitimes
  - **Chiffrement des flux** pour empêcher l'analyse des signaux et les attaques de type homme du milieu

Prise de contrôle d'un véhicule automobile

Impact

Prise de contrôle d'un véhicule, obligation de rappel des véhicules (1,4 millions de véhicules)

Scénario d'incident

Prise de contrôle du véhicule par deux chercheurs

Vulnérabilité

Réseau WiFi avec clé prédictible et **vulnérabilités d'un contrôleur attaché au CAN bus** (réseau interne interconnectant les fonctions du véhicule)

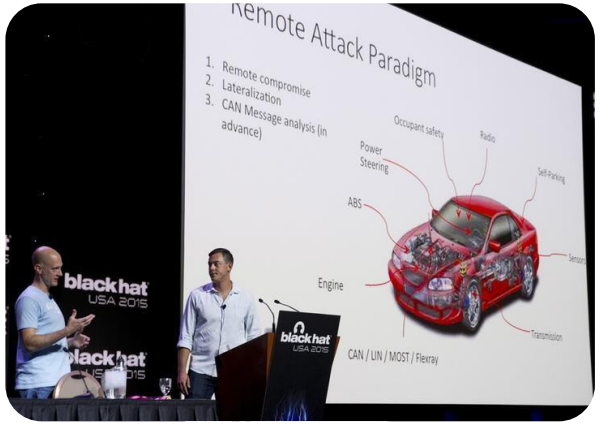
Prise de contrôle d'un véhicule automobile

Club de la sécurité de l'information français

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 mis en œuvre

- Deux personnes avec de très bonnes connaissances techniques
- Une antenne GSM achetée sur ebay
- Un nouveau firmware créé par 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 système 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…)

2015	Transport	Saint Louis, USA	Wired

Perturbation des systèmes de signalisation ferroviaire -SoBig & Blaster

Impact

Perturbations du trafic ferroviaire pendant une journée dans l'Est des États-Unis

Scénario d'incident

Attaque simultanée de deux virus (SoBig.F et Blaster) sur les systèmes de contrôle de CSX Corporation (compagnie ferroviaire américaine) entrainant leur indisponibilité

Vulnérabilité

Failles de sécurité dans Windows, non détection du virus par les antivirus, utilisation de mails frauduleux

Perturbation des systèmes de signalisation ferroviaire -SoBig & Blaster

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Ludique	Moyenne

Déroulement de l'attaque

- Le système de contrôle a été infecté par les virus, entrainant le ralentissement puis **l'arrêt des applications de pilotage de la signalisation et de communication ferroviaire.**
- Le trafic des trains a été perturbé
- La neutralisation puis le redémarrage des services a toutefois été rapide (journée)

Moyens mis en œuvre

•Le virus SoBig s'est propagé entre 2002 et 2003 en exploitant une faille de sécurité dans Windows, et par l'usage de courriels frauduleux

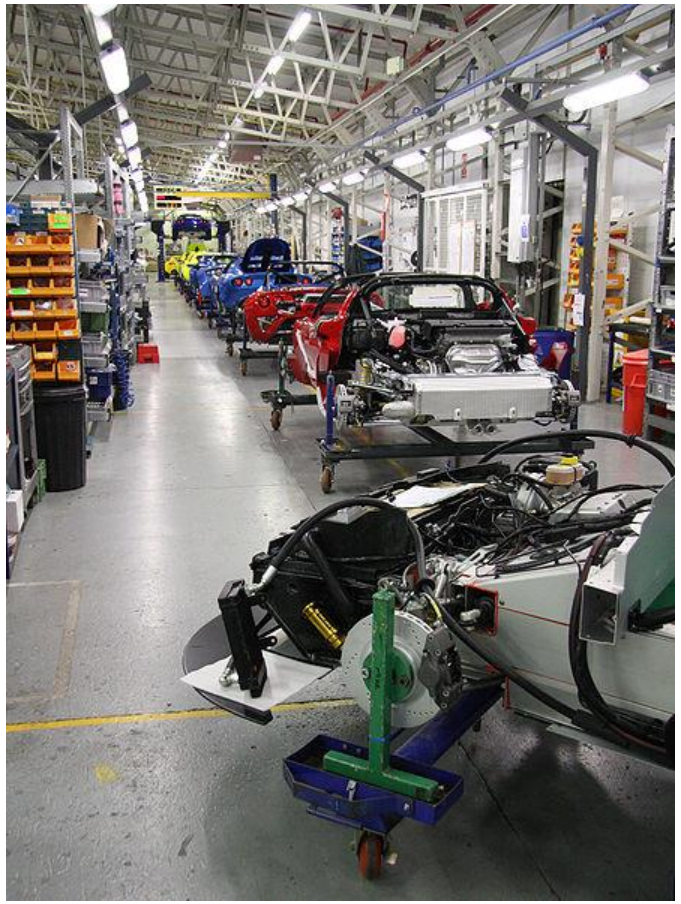
•Le virus Blaster s'est propagé en 2003 et générait des attaques par déni de service

•Investissement financier faible

Enseignement à tirer, préconisation et contre-mesures

- Les mesures suivantes auraient permis de s'en prémunir ou d'en limiter la portée:
  - **Sensibilisation** des utilisateurs sur les mails frauduleux et les techniques de propagation, utilisation des antivirus pour vérifier les pièces jointes aux courriels.
  - **Mise à jour des bases d'antivirus**
  - Neutralisation des serveurs infectés par les opérateurs de télécommunication ou par les hébergeurs
  - **Sécurisation des applications de bureautique** (Office…) pour limiter toute tentative de propagation de virus

Déni de service sur usines automobiles - Zotob



Impact

13 usines arrêtées pendant environ 1 heure, 50.000 travailleurs (14 M$ de dommages)

Scénario d'incident

Propagation d'un ver sur la chaîne de montage

Vulnérabilité

Manque de filtrage au niveau de l'interconnexion du réseau industriel avec le réseau bureautique

Déni de service sur usines automobiles - Zotob

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Moyenne	Attaque indifférenciée	Faible

Déroulement de l'attaque

- Le ver **Zotob**, découvert en 2005, se diffuse sur Internet en exploitant des vulnérabilités présentes dans le protocole PnP. Les systèmes affectés par ce ver sont les machines Windows (Windows 2000 non patchés en particulier) connectées en réseau.
- Les serveurs Windows 2000 de DaimlerChrysler ont été victimes de cette vague d'infection.
- Malgré un **firewall** entre les réseaux d'entreprise et industriel, le ver s'est retrouvé sur **les systèmes industriels**. Il s'est **propagé entre les usines**, les rendant indisponibles.

Moyens mis en œuvre

- Un ver (Zotob)
- Des services exposés vers l'externe
- Des réseaux interconnectés

Enseignement à tirer, préconisation et contre-mesures

- Un système critique doit être suffisamment **cloisonné** pour limiter la propagation des attaques.
- Les mesures suivantes auraient permis de s'en prémunir :
  - **Défense en profondeur** et **cloisonnement strict** des systèmes liés à la production (isolation physique, diode, protection hardware)
  - **Limitation des services exposés vers l'externe** : durcissement de systèmes, filtrages des flux autorisés

Prise de contrôle du système de production d'une aciérie

Impact

Lourds dégâts matériels causés par la perte de contrôle des logiciels de production

Scénario d'incident

Prise de contrôle du système de contrôle de l'usine par **« spear phishing »** via le réseau bureautique

Vulnérabilité

Passerelle entre le réseau de production et le réseau bureautique

Prise de contrôle du système de production d'une aciérie

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Financier ou Terroriste	Élevée

Déroulement de l'attaque

- Les hackers se sont d'abord introduits sur le réseau bureautique du site industriel par la technique du **« spear phishing »** (campagne de mails infectés).
- Depuis ce premier réseau, ils ont pénétré les logiciels de gestion de production de l'aciérie, puis pris les commandes de la plupart des systèmes de contrôle de l'usine.
- Ils ont alors empêché un haut fourneau de se mettre en sécurité à temps et causé de gros dégâts à l'infrastructure.

Moyens mis en œuvre

- Un groupe d'individus expérimentés ayant une bonne connaissance des systèmes industriels
- Investissement financier important

Enseignement à tirer, préconisation et contre-mesures

- La méthode d'attaque par « spear phishing » requiert des moyens importants et de bonnes connaissances des systèmes ciblés, mais s'avère d'une efficacité redoutable.
- Les mesures suivantes auraient permis de s'en prémunir ou d'en limiter les effets:
  - **Sensibilisation** des agents aux méthodes d'attaque par « spear phishing »
  - **Restriction des droits accordés aux profils d'agent** sur le réseau et les systèmes, de façon à détecter voire empêcher toute action suspecte (prise de contrôle de systèmes, de terminaux…)
  - **Cloisonnement des réseaux** de bureautique, exposés aux attaques et aux intrusions, et des réseaux de contrôle des systèmes de production
  - Mise en place de mécanismes de sûreté **indépendant** du système de conduite

2014 | Industrie | Allemagne | BSI, Arstechnica

Divulgation de documents d'une centrale nucléaire

Impact

Publication de documentation technique sur les réacteurs et **d'informations sur le personnel** de la KHNP (Korea Hydro & Nuclear Power)

Scénario d'incident

Infection des comptes des employés de KHNP

Vulnérabilité

Négligence du personnel

Divulgation de documents d'une centrale nucléaire

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Faible	Politique / Financière	Moyenne

Déroulement de l'attaque

- Après une **campagne de « spear phishing »** (campagne de mails infectés) qui a touché **3571 employés**, l'attaquant a pu avoir accès aux différents documents de KHNP.
- L'attaquant **a publié les documents sur twitter** en plusieurs temps se faisant passer pour le vice-président d'une association anti-nucléaire et a conseillé les personnes habitant près des centrales de quitter les lieux.
- L'attaquant a aussi demandé **une rançon** pour la non publication des documents.
- Il semblerait que l'attaquant ait **essayé d'attaquer le système industriel** mais n'a pas réussi.

Moyens mis en œuvre

- Campagne de hameçonnage ciblé
- Kimsuky est un logiciel malfaisant supposé utilisé par la Corée du Nord

Enseignement à tirer, préconisation et contre-mesures

- Les employés n'étaient pas assez **sensibilisés** aux différentes menaces, attaques par « spear phishing ».
- Les mesures suivantes auraient permis de s'en prémunir:
  - Mener une **campagne de sensibilisation**
  - **Classifier les informations** de l'entreprise
  - Adapter le niveau de sécurité selon le **niveau de confidentialité des données** (Chiffrement, restriction d'accès, traçabilité)
- Point positif : Après l'attaque, KHNP a fait **un exercice** pour vérifier sa capacité à faire face à une attaque cyber.

Sabotage d'un processus industriel - Stuxnet

2009-2010 | Nucléaire | Natanz, Iran | Fiche 18

Impact

Retard de **6 mois à 1 an** du programme nucléaire iranien, **plusieurs millions d'euros** de matériel endommagés (principalement dans la centrale de Natanz)

Scénario d'incident

Logiciel malveillant avancé (nommé **Stuxnet**), injecté sur un poste SI de gestion, et ayant circulé jusqu'au SI industriel

Vulnérabilité

Absence de contrôle clé USB, **pas de segmentation** ni de détection d'intrusion sur SI industriels, **PC non durcis**, équipements industriels avec **vulnérabilités ignorées**

Sabotage d'un processus industriel - Stuxnet

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Majeure	Stratégique inter-états	Très Élevée

Déroulement de l'attaque

- Après une importante **phase d'espionnage** des installations nucléaires Iraniennes, et d'importants travaux de **recherche et développement**, les attaquants ont réussi à développer le virus **Stuxnet**.
- Stuxnet était en mesure de **se répliquer et circuler sans action nocive**, jusqu'à la cible (contrôle-commande centrifugeuses).
- Arrivé sur SI de gestion, il a pu se diffuser vers le SI industriel **même en l'absence d'interconnexion réseau** (via USB ou PC portable).
- La « charge active » (code automate) était très complexe, faisant dériver le processus de manière **peu détectable**, avec pour conséquence d'user prématurément les centrifugeuses, composants mécaniques très sensibles à certaines fréquences de résonance. Cette charge n'était activée que lorsqu'elle était en contact avec l'automate.

Moyens mis en œuvre

Organisation mandatée par les USA en partenariat avec Israël :

- atelier « génie logiciel » dédié au développement de Stuxnet :
  - 15 exploits
  - 4 0-day
- espionnage
- complicité locale interne

Enseignement à tirer, préconisation et contre-mesures

- La protection par **isolation de réseau** (« air-gap ») n'est plus efficace. De plus l'attaque a été révélatrice des **capacités d'attaques d'un état**.
- Les mesures suivantes auraient permis de s'en prémunir :
  - **Protection des informations** (architecture, codes) des processus industriels.
  - Prise en compte des exigences de cybersécurité lors de la **conception des équipements et applications industriels**. Ils comportent en effet de très nombreuses « failles » souvent sans solution.
  - **Développement de tous les axes de défense** : segmentation (réseaux, droits, infos), détection, durcissement, gestion des vulnérabilités…

2009	Nucléaire	Natanz, Iran	Ralph Langer Blog, NY Times

Infection par ver dans une centrale nucléaire - Slammer

Impact

6 heures d'indisponibilité de la centrale de Davis-Besse, systèmes de sûreté inopérants

Scénario d'incident

Propagation d'un ver via un réseau de communication privé

Vulnérabilité

Interconnexion entre un réseau de communication privé et les systèmes industriels

Infection par ver dans une centrale nucléaire - Slammer

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Moyenne	Attaque indifférenciée	Faible

Déroulement de l'attaque

- Durant Janvier 2003, le ver Slammer a infecté plusieurs serveurs Microsoft SQL 2000 dans le monde causant ainsi un important **déni de service**.
- Dans un premier temps, le ver avait infecté le serveur d'un prestataire de la centrale. Ce poste possédait une connexion de type T1 le liant directement au SI industriel **contournant le pare-feu** séparant ce dernier du SI de gestion.
- Le ver a alors envoyé plusieurs paquets sur le réseau industriel le **surchargeant** et **rendant ainsi indisponible le système de sûreté** (safety parameter display system (SPDS)) et le poste de contrôle de la centrale.

Moyens mis en œuvre

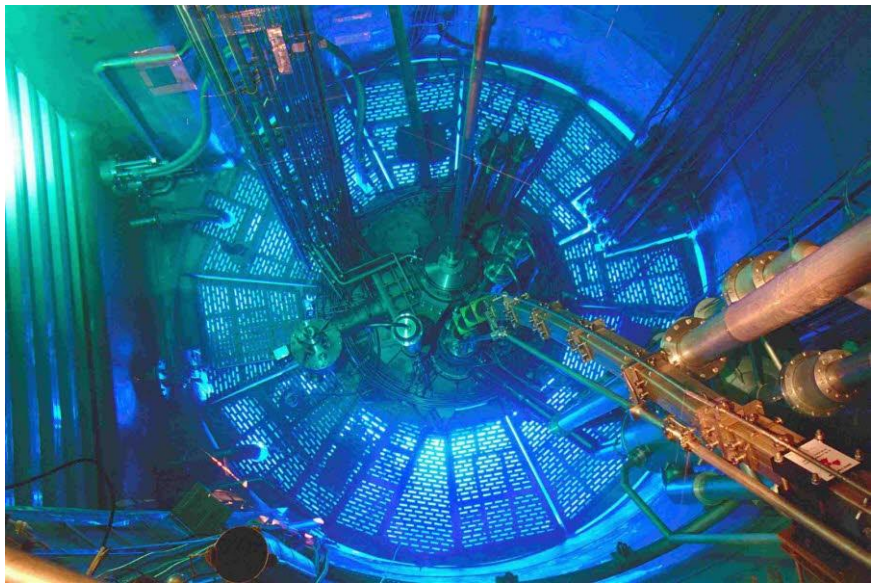
- Un ver (Slammer)
- Des services exposés vers l'externe
- Des réseaux interconnectés

Enseignement à tirer, préconisation et contre-mesures

- Une connaissance des différentes connexions existantes entre le réseau industriel, le SI de gestion et les réseaux externes est nécessaire pour mettre en place les infrastructures de défense appropriées.
- Les mesures suivantes auraient permis de s'en prémunir :
  - **Cartographie du SI** avec un cloisonnement strict du réseau industriel et des systèmes liés à la sûreté (isolation physique, diode, protection hardware)
  - **Limitation des services exposés vers l'externe** : durcissement de systèmes, filtrages des flux autorisés
  - **Application des patchs de sécurité**

2003 | Nucléaire | Ohio, USA | Security Focus

Arrêt d'urgence d'un réacteur nucléaire



Impact

Arrêt d'un réacteur nucléaire

Scénario d'incident

Une mise à jour réinitialise les données du système de contrôle

Vulnérabilité

Mauvaise intégration de « Composants pris sur étagère » (COTS) avec des systèmes de contrôle industriels

Arrêt d'urgence d'un réacteur nucléaire

Club de la sécurité de l'information français

Gravité	Motivation	Complexité
Moyenne	Erreur	Faible

Déroulement de l'incident

- Un ingénieur installe une mise à jour d'un logiciel présent sur un poste du SI de gestion de la centrale. Ce poste permettait d'analyser les données envoyées par le SCADA. **La mise à jour a été conçue pour synchroniser les deux systèmes d'informations.**
- Après la mise à jour**, le redémarrage du système réinitialise les données du système de contrôle**.
- Les dispositifs de sûreté interprètent les données erronées et concluent à une fuite de la « piscine ».
- Le réacteur nucléaire se met en arrêt d'urgence.

Moyens mis en œuvre

- Une seule personne en charge des interfaces SCADA de surveillance
- Un logiciel inadapté ou mal intégré
- Des procédures non sécurisées

Enseignement à tirer, préconisation et contre-mesures

- Lorsque les réseaux sont mal cloisonnés, **une mise à jour légitime des systèmes peut mettre en danger le SI Industriel**.
- Les mesures suivantes auraient permis de s'en prémunir:
  - Établissement d'un **protocole de mise à jour des logiciels**
  - **Cloisonnement du SI industriel critique**, et particulièrement les serveurs de données
  - **Communication avec les éditeurs de logiciel** pour déterminer les possibles répercussions que peut avoir une mise à jour de logiciel sur le SI
  - **Réalisation de tests de mises à jour** sur des systèmes hors-production avant leur application en production

2008 | Nucléaire | USA | Washington Post

Détournement d'un drone de reconnaissance

Impact

Récupération d'un drone « Sentinel » américain permettant le retro-engineering et copie

Scénario d'incident

Détournement via **émission de faux signaux GPS** leurrant le drone mais également le contrôle à distance

Vulnérabilité

Manque de sécurisation du système GPS

Détournement d'un drone de reconnaissance

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Vol d'information (plans…)	Élevée

Déroulement de l'attaque

- Analyse du fonctionnement de la navigation et du pilotage à distance de drones plus anciens (accidentés).
- Attaque en deux étapes une fois un drone dans le périmètre des émetteurs :
  - **Brouillage des communications** du pilotage à distance : le drone passe en mode « auto-pilote » et va atterrir à sa base
  - **Modification du signal GPS** pour que sa « base » coïncide avec une piste sur le territoire iranien.

Moyens mis en œuvre

- Retro-engineering de drones.
- Brouillage des communications et émission de faux signaux GPS avec suffisamment de puissance pour leurrer un drone en vol.

Enseignement à tirer, préconisation et contre-mesures

- La **vulnérabilité était connue** (selon Christian Science Monitor) par l'armée américaine, et le risque mal évalué (ou non identifié) : une **gestion des risques** basée sur une identification des vulnérabilités est indispensable.
- Le signal GPS doit être considéré comme **non-fiable** pour des applications critiques.
- La cybersécurité doit être prise en compte dans les modes dégradés des systèmes de conduite.

Attaque de terminaux de points de vente – BlackPOS

Impact

40 millions de numéros de cartes bancaires détournés, **70 millions de comptes clients piratés de Target** (chaîne de grande distribution), dévalorisation boursière, licenciement du directeur général (CEO)

Scénario d'incident

Compromission des terminaux de point de vente par un **cheval de Troie**

Vulnérabilité

Accès à distance non protégé pour la maintenance de la climatisation

Attaque de terminaux de points de vente – BlackPOS

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Majeure	Financière	Élevée

Déroulement de l'attaque

- Les attaquants ont lancé une attaque ciblée pour récupérer les paramètres de connexion (nom d'utilisateur/ Mot de passe) de l'**accès à distance d'un prestataire de maintenance du système de climatisation.**
- **Ils ont alors pu s'introduire sur les PoS** (Points of sales) **par rebond sur le réseau industriel,** afin d'**installer le malware** (BlackPOS) pour intercepter **à la volée les codes des cartes bancaires.** Le malware se chargeait de déposer ces données **sur un serveur interne compromis.**
- Enfin, **les données bancaires** récupérées auparavant ont été exfiltrées vers un **serveur FTP extérieur** (localisé en Russie) avant d'être mises en vente sur Internet.

Moyens mis en œuvre

- Ingénierie sociale par email avec PJ infectée (« *spear phishing* »)
- Utilisation du malware BlackPOS, de type RAM-scraping (trojan)

Enseignement à tirer, préconisation et contre-mesures

- La **gouvernance** globale de la cybersécurité de l'entreprise doit intégrer **la gestion technique des bâtiments**.
- Les mesures suivantes auraient permis de s'en prémunir :
  - Mise en place d'une protection efficiente au-delà de la simple conformité à la règlementation (Target venait d'être certifié PCI-DSS)
  - Mise en place d'une **authentification forte** au niveau des accès à distance (accès standard sur le système externe de facturation)
  - Mise en place d'un **cloisonnement du réseau** afin préserver les zones sensibles (déplacement horizontal jusqu'au réseau industriel)
  - Mise en place d'une **veille technique** sur les failles découvertes sur les PoS (bulletin d'alerte publié par Visa plusieurs mois auparavant)
  - Mise en place d'une **cybersurveillance du SI** visant à gérer les alertes remontées par les dispositifs de détections (alertes FireEye ignorées)

2013 | Distribution | USA | Rapport Senat Americain : A kill chain analysis

Attaque sur une pompe à insuline

Impact

Modification potentielle des doses d'insuline

Scénario d'incident

Altération et envoi de commandes radio

Vulnérabilité

Données non chiffrées et manque d'authentification des sondes

Attaque sur une pompe à insuline

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Faible	Sensibilisation	Moyenne

Déroulement de l'attaque

- Après l'analyse de la documentation constructeur (manuel d'utilisation, analyse des brevets, numéro de série de l'appareil…) un chercheur est parvenu à **intercepter les communications** échangées entre les capteurs et sa pompe à insuline.
- L'analyse des logs a montré que la pompe utilisait entre autre une application JAVA **non obfusquée** qui pilote l'équipement. Le chercheur a alors pu établir la liste des **codes de commande utiles de l'équipement**.
- Le chercheur a imaginé plusieurs scénarios d'attaques : **rejeu** de valeurs transmises à la pompe par les sondes, **envoi de commandes forgées** directement à la pompe (accès physique requis pour connaître le numéro de série nécessaire à l'envoi).

Moyens mis en œuvre

- Antenne radio (pour moins de 100€ sur ebay).
- Connaissances des outils et technologies « radio »

Enseignement à tirer, préconisation et contre-mesures

- Les objets connectés présentent plusieurs vulnérabilités liées au **manque d'intégration de la sécurité lors de leur conception**. De plus, les équipements autonomes **ne présentent pas de système de sécurité (safety)** comme dans les systèmes industriels classiques rendant une attaque potentiellement plus dangereuse.
- Les mesures suivantes permettent de sécuriser ce types d'équipements de santé :
  - Forcer **l'authentification mutuelle** des sondes et pompes à insuline ;
  - **Chiffrer** les signaux échangés ;
  - En conclusion: intégrer la **sécurité dans la phase de conception** de ces objets.

Club de la sécurité de l'information français

Présentation du CLUSIF

Club de la sécurité de l'information français

Présentation du CLUSIF

- Association à but non lucratif réunissant des professionnels de la sécurité
  - Plus de 250 sociétés membres
  - 15 secteurs de l'économie représentés
  - Offreurs et Utilisateurs réunis de manière équilibrée

- Échanger et agir ensemble pour la confiance dans le numérique
  - Élaborer et transmettre un ensemble de bonnes pratiques en matière de sécurité de l'information au travers :
    - Des groupes de travail
    - Des publications
    - Des conférences thématiques

Les activités de l'association

- Groupes de travail
  - Réunissent mensuellement des Utilisateurs et des Offreurs autour de problématiques données
  - Ont pour finalité la rédaction puis la publication d'un document de type Livre Blanc, Guide de Bonnes Pratiques, Recommandations ou État de l'art
- Publications
  - Mise à disposition (gratuitement) sur le site Web du CLUSIF de l'ensemble des documents produits par les groupes de travail de l'association
- Conférences
  - 5 conférences thématiques par an pour sensibiliser à l'importance de la sécurité de l'information

Un espace unique dédié aux RSSI

- L'Espace RSSI du CLUSIF, un lieu d'échange privilégié
  - Réservé aux Responsables Sécurité Informatique d'entreprises privées et du secteur public (hors fournisseurs de solutions ou de services de sécurité)
  - Favorise l'échange de savoir-faire et de retours d'expériences autour :
    - De problématiques rencontrées
    - De solutions mises en œuvres
    - De nouvelles normes
    - De nouvelles réglementations et obligations juridiques
  - Interventions ponctuelles d'organismes institutionnels
  - Réunions mensuelles, généralement le vendredi en début de chaque mois

Pour plus d'information

- Site Web de l'association
  www.clusif.fr

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

Crédit Photos

Club de la sécurité de l'information français

Crédit photos

- Synthèse:
  - http://www.mintincorp.com/industrial-sector/oil-gas/
- Interruption de production d'électricité – slide 1:
  - https://upload.wikimedia.org/wikipedia/commons/4/42/Hydrolienne_Sabella_D10_%284%29.JPG
- Interruption de production d'électricité – slide 2:
  - http://www.techworld.com/security/surviving-ransomware-kaspersky-lab-offers-advice-on-coping-with-extortion-attack-3626776/
- Attaque d'une station d'épuration des eaux - slide 1:
  - https://commons.wikimedia.org/wiki/File%3AWWTP_Antwerpen-Zuid.jpg
- Attaque d'une station d'épuration des eaux - 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
- Prise de contrôle de l'aiguillage d'un tramway - 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
- Prise de contrôle de l'aiguillage d'un tramway - slide 2:
  - https://www.wired.com/2008/01/polish-teen-hac/
- Divulgation de documents d'une centrale nucléaire - slide 1:
  - https://commons.wikimedia.org/wiki/File%3ACANDU_at_Qinshan.jpg
  - Atomic Energy of Canada Limited [Attribution], via Wikimedia Commons
- Divulgation de documents d'une centrale nucléaire - slide 2:
  - https://commons.wikimedia.org/wiki/File%3AWolsong_(04790183).jpg
  - By IAEA Imagebank (Flickr: 04790183) [CC BY-SA 2.0 (http://creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons
- Déni de service sur usines automobiles - Zotob - slide 1:
  - https://commons.wikimedia.org/wiki/File%3AFinal_assembly_3.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
- Déni de service sur usines automobiles - 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
- Mise hors service d'un superviseur de dérivation d'eau - slide 1:
  - http://www.water-technology.net/projects/delta-mendota-canal-california-aqueduct-intertie/delta-mendota-canal-california-aqueduct-intertie1.html
- Mise hors service d'un superviseur de dérivation d'eau - slide 2:
  - Anthony DUNN
  - http://www.adunnphotography.com/media/55fc9b6b-d79d-40c7-883d-cbe6857ebebb-tehama-colusa-canal-1
- Attaque de terminaux de points de vente - BlackPOS – slide 1:
  - https://commons.wikimedia.org/wiki/File%3ATarget_West_Reynolds_Road_Lexington%2C_KY_3_(9568771360).jpg
  - By Mike Kalasnik from Fort Mill, USA [CC BY-SA 2.0 (http://creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons
- Attaque de terminaux de points de vente - BlackPOS – slide 2:
  - https://blog.kissmetrics.com/gamification-for-better-results/
- Sabotage d'un processus industriel – Stuxnet – slide 1:
  - https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
- Sabotage d'un processus industriel – Stuxnet – slide 2:
  - https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
- Infection par ver dans une centrale nucléaire - Slammer – slide 1:
  - https://commons.wikimedia.org/wiki/File%3ADavid_Besse_NPP-2.jpg
  - By David_Besse_NPP.jpg: Nuclear Regulatory Commission.Theanphibian at en.wikipedia derivative work: Saibo (Δ) (David_Besse_NPP.jpg) [Public domain], from Wikimedia Commons
- Infection par ver dans une centrale nucléaire – Slammer – slide 2:
  - https://commons.wikimedia.org/wiki/File%3ADavis-Besse_Nuclear_Power_Station_cooling_tower_(4183).jpg
  - By Gregory Varnum (Own work) [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons
- Déversement d'eaux usées - slide 1:
  - http://traitementdeseaux.fr/eaux-industrielles/
- Déversement d'eaux usées - slide 2:
  - http://www.eham.net/classifieds/detail/335053
- Explosion d'un pipeline – slide 1 :
  - https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar
- Explosion d'un pipeline – slide 2 :
  - https://commons.wiki
  - 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
- Prise de contrôle d'un véhicule automobile - slide 1:
  - https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
- Prise de contrôle d'un véhicule automobile - slide 2:
  - http://in.reuters.com/article/us-cybersecurity-autos-senators-idINKCN0RG2B420150916
- Destruction d'un système d'information – Shamoon – slide 1:
  - http://www.gulfeyes.net/saudi-arabia/503401.html
- Destruction d'un système d'information - Shamoon – slide 2:
  - https://www.theguardian.com/business/2011/jul/31/vedanta-resources-cairn-energy-india-deal
- Détournement d'un drone de reconnaissance – slide 1:
  - http://www.defensetech.org/2011/12/08/iranian-tv-shows-captured-rq-170/
- Détournement d'un drone de reconnaissance – slide 2:
  - https://commons.wikimedia.org/wiki/File%3ARQ-170_Wiki_contributor_3Dartist.png
  - © TruthDowser / Wikimedia Commons, در ویکی‌انبار
- Prise de contrôle du système de production d'une aciérie - slide 1:
  - http://www.france-metallurgie.com/portrait-de-lacierie-badische-stahlwerke/
- Prise de contrôle du système de production d'une aciérie - slide 2:
  - http://www.bbc.com/news/technology-30575104
- Perturbation des systèmes de signalisation ferroviaire - Sobig/Blaster - slide 1:
  - http://www.forbes.com/pictures/fjle45jhgk/the-top-50-military-friendly-employers/#17c8ea971daf
- Perturbation des systèmes de signalisation ferroviaire - Sobig/Blaster - slide 2:
  - http://toastytech.com/guis/win98.html
- Coupure d'électricité en 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)
- Coupure d'électricité en 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/
- Exfiltration de données de compagnies d'énergie - slide 1:
  - http://www.alalam.ir/news/1648514
- Exfiltration de données de compagnies d'énergie - slide 2:
  - http://www.federaltimes.com/story/government/cybersecurity/2016/06/14/apt28-sofacy-us-officials/85866698
- Compromission du réseau informatique - slide 1:
  - http://www.huffingtonpost.ca/2012/09/28/calgary-telvent-security--hacking-chinese_n_1924078.html
- Compromission du réseau informatique - slide 2:
  -
- Explosion d'un gazoduc - slide 1 :
  - http://www.euractiv.com/section/europe-s-east/news/ukraine-suspects-russian-foul-play-behind-pipeline-blast/
- Explosion d'un gazoduc - slide 2 :
  - https://southfront.org/main-gas-pipeline-stavropol-moscow-was-blown-up-near-the-city-rovenki/
- Empoisonnement de l'eau potable – slide 1:
  - http://kitprofs.com/services/water/
- Empoisonnement de l'eau potable – slide 2:
  - https://www.compricer.se/nyheter/artikel/sparpengar-ar-skyddade-av-insattningsgarantin--men-hur-ar-det-med-fonder-och-aktier
- Arrêt d'urgence d'un réacteur nucléaire – slide 1:
  - http://www.ledauphine.com/actualite/2011/03/14/un-(petit)-reacteur-nucleaire-a-grenoble
- Arrêt d'urgence d'un réacteur nucléaire – slide 2:
  - http://courrierstrategique.com/4899-russie-construction-des-reacteurs-nucleaires-en-iran.html
- Attaque sur une pompe à insuline – slide 1:
  - http://discovermagazine.com/2016/may/13-priming-the-pump
- Attaque sur une pompe à insuline – slide 2:
  - http://www.startribune.com/supreme-court-won-t-block-medtronic-liability-case/264836081/
- Credit icones:
  - http://flaticon.com