



FICHES INCIDENTS CYBER SI INDUSTRIELS

**GROUPE DE TRAVAIL CYBERSÉCURITÉ DES SYSTÈMES
INDUSTRIELS**

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 :

Hervé	SCHAUER	<i>HS2</i>
Ilias	SIDQUI	<i>Wavestone</i>

Les contributeurs de cette seconde édition :

Christophe	AUBERGER	<i>Fortinet</i>	David	DIALLO	<i>ANSSI</i>
Guillaume	CHAUSSIN	<i>Cisco</i>	Benoît	GRAND-PERRIN	<i>GE</i>
Cédric	ESCALLIER	<i>Suez</i>			
Guillaume	LE HEGARET	<i>Setec ITS</i>			

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

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

SOMMAIRE

Présentation du groupe de travail « Cybersécurité des systèmes industriels »	5
Présentation du document	7
Objectifs	8
Démarche adoptée	9
Comment lire les fiches ?	11
Sommaire des incidents analysés	13
Analyse des incidents	18
Synthèse	23
Quelles tendances pour les années à venir ?	24
Fiches incidents	25
Présentation du CLUSIF	120
Crédit photo	124

PRÉSENTATION DU GROUPE DE TRAVAIL “CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS”

GT Cybersécurité des systèmes industriels

Le groupe de travail Cybersécurité des systèmes industriels 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 plusieurs publications :

- Le *Panorama des référentiels de sécurité*, dont la mise à jour a été publiée en 2019 ;
- Le *Guide cybersécurité des systèmes industriels*, publié en 2021.

En 2017, le GT a publié « Fiches incidents Cyber SI industriel » dont ce document est la seconde édition.





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 concepts pour leur dimension didactique.
- Outre les responsables de la 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 interagir avec 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.

Le périmètre 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 d'incidents cyber.

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



2

Sélection

Les incidents sélectionnés 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 ses 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.**

Les incidents provoqués par un rançongiciel ont fait l'objet d'un traitement spécifique détaillé par la suite.



3

Restitution

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

Chaque fiche est constituée de deux pages :

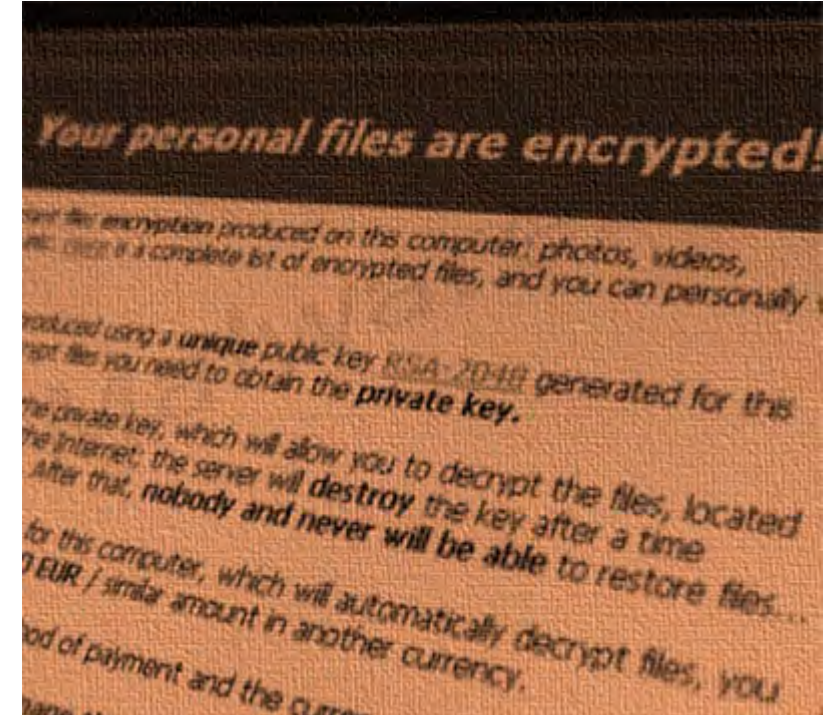
- **Un visuel** et une **description synthétique de l'attaque** ;
- Le **déroulé et les impacts** basés sur les sources préalablement identifiées ainsi que les **recommandations du Clusif**.

INCIDENTS INDUSTRIELS ET RANÇONGIELS

La veille effectuée par les membres du GT a permis d'identifier de nombreux incidents industriels dus aux rançongiciels.

Les sources publiques ayant reporté les faits d'incidents causés par un rançongiciel ne détaillent pas le scénario de compromission (mécanismes d'intrusion dans le système d'information, vulnérabilités exploitées, etc.).

Ainsi, il a été noté que les informations reportées par les sources publiques diffèrent rarement d'un incident à l'autre. Il a donc été décidé de ne pas réaliser de fiche dédiée pour chaque incident causé par un rançongiciel à l'exception de NotPetya, Wannacry et deux incidents affectant des dispositifs spécifiques (téléphérique ou dispositif de contrôle d'accès physique, par exemple).



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

PRISE DE CONTRÔLE D'UN VÉHICULE AUTOMOBILE

2015 Transport Saint louis, USA Fiche 23

Impact

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

Scénario d'incident

Prise de contrôle du véhicule par deux chercheurs

Vulnérabilité

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



COMMENT LIRE LES FICHES? 2/2

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

- Faible : pas ou peu d'impact ;
- Moyenne : perte de production ponctuelle, pas d'impacts humains, pas d'impacts écologiques ;
- 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.

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

PRISE DE CONTR LE D'UN V HICULE AUTOMOBILE

CLUSIF

Gravit  de l'attaque: Faible, Moyenne,  lev e

Motivation de l'attaquant:  conomique

Complexit  de l'attaque: Faible, Moyenne,  lev e, Tr s  lev e

D roulement de l'attaque

Certaines voitures sont  quipp es d'une option permettant au conducteur de contr ler la console de bord par Wi-Fi. Les chercheurs ont r uss , en d couvrant la cl  Wi-Fi,   s'introduire dans le r seau sans fil. Ils ont pris le contr le de la console de bord en exploitant ses vuln rabilit s.

- Les v hicules du m me mod le sont connect s au r seau GSM. En utilisant une antenne GSM, les chercheurs ont r uss    acc der   distance   la console de bord.
- Cette console est connect e au CAN bus (r seau interne interconnectant les fonctions du v hicule),   travers un autre composant, le V850.
- En modifiant le firmware du V850, les chercheurs ont envoy  des commandes au v hicule.

Enseignements   tirer, pr conisations et contre-mesures

- Comme pour les SI industriels, les v hicules doivent cloisonner les fonctions vitales/importantes de transport des fonctions de divertissement. L'acc s au syst me informatique du v hicule doivent  tre prot g s :
 - La cl  Wi-Fi ne doit pouvoir  tre pr dictible (date de sortie de l'usine)
 - Des m canismes de contr le d'acc s doivent permettre de prot ger les v hicules contre des actions non autoris es.
- Les mesures suivantes auraient permis de s'en pr munir :
 - Utilisation d'un algorithme assurant une g n ration de cl  non pr dictible ;
 - Mise en place d'un m canisme emp chant la mise   jour du Firmware du contr leur V850 par un code non sign  ;
 - Filtrage des communications entre le contr leur V850 et le CAN bus (ACL, pare-feu...)

2415 Transport Saint Louis, USA Wired

La complexit  de l'attaque d pend des moyens mis en  uvre. Quatre niveaux de complexit  ont  t  identifi s :

- Faible : pas d'outil n cessaire ;
- Moyenne : outillage n cessaire, comp tence technique simple   acqu rir par l'attaquant ;
-  lev e : outillage n cessaire, comp tences techniques fortes et sp cifiques ;
- Tr s  lev e : d veloppement sp cialis  pour l'attaque avec des moyens financiers et humains tr s importants.

Rappel du contexte

Quelque(s) source(s) utilis e(s) pour l' laboration de la fiche

INCIDENTS ANALYSÉS

Fiche 0	Attaques par Rançongiciel	Monde	
Fiche 1	Rançonnage des services de santé britanniques WannaCry	Royaume-Uni	2017
Fiche 2	Attaque d'ampleur mondiale – notPetya	Monde	2017

Énergie

Fiche 3	Interruption de production d'électricité	France	2015
Fiche 4	Coupure générale d'électricité – BlackEnergy	Ukraine	2015
Fiche 5	Exfiltration de données de compagnies d'énergie – Havex	Europe/USA	2013-2014
Fiche 6	Compromission du réseau informatique	Canada	2012
Fiche 7	Arrêt automatique de processus industriel – Triton	Arabie saoudite	2017
Fiche 8	Prise de contrôle d'éolienne	USA	2017
Fiche 9	Déni de service sur un chauffage public - Mirai	Finlande	2016
Fiche 10	Attaque sur un réseau éolien et solaire	USA	2019
Fiche 11	Rupture du transport d'énergie électrique – Crashoverride/Industroyer	Ukraine	2016

INCIDENTS ANALYSÉS

Pétrole & Gaz



Fiche 12	Explosion d'un pipeline	Turquie	2008
Fiche 13	Destruction d'un système d'information – Shamoon	Arabie saoudite	2012
Fiche 14	Explosion d'un gazoduc	URSS	1982
Fiche 15	Vol de carburant en station-service	Israël	2018

Eau/assainissement



Fiche 16	Attaque d'une station d'épuration des eaux	N/C	2015
Fiche 17	Mise hors service d'un superviseur de dérivation d'eau	USA	2007
Fiche 18	Déversement d'eaux usées	Australie	2000
Fiche 19	Empoisonnement de l'eau potable	USA	2013
Fiche 20	Minage de cryptomonnaie Monero	Europe	2018
Fiche 21	Modification des paramètres d'une station de traitement d'eau	USA	2021

INCIDENTS ANALYSÉS

Transport



Fiche 22	Prise de contrôle de l'aiguillage d'un tramway	Pologne	2008
Fiche 23	Prise de contrôle d'un véhicule automobile	USA	2015
Fiche 24	Perturbation des systèmes de signalisation ferroviaire – Sobig/Blaster	USA	2003
Fiche 25	Démonstrateur d'une attaque d'une station de lavage automobile	USA	2017
Fiche 26	Compromission d'un véhicule	Monde	2017
Fiche 27	Ouverture d'un véhicule	USA	2017
Fiche 28	Brouilleur GPS bloquant un aéroport	France	2017
Fiche 29	Leurre de GPS	Chine	2019
Fiche 30	Blocage d'un téléphérique par des hackers	Russie	2018

INCIDENTS ANALYSÉS

Industrie



Fiche 31	Déni de service sur usines automobiles – Zotob	USA	2005
Fiche 32	Prise de contrôle du système de production d'une aciérie	Allemagne	2014
Fiche 33	Perturbation du système de production par vengeance	USA	2014
Fiche 34	Tentative de perturbation des installations frigorifiques	France	2019

Nucléaire



Fiche 35	Divulgence de documents d'une centrale nucléaire	Corée du Sud	2014
Fiche 36	Sabotage d'un processus industriel – Stuxnet	Iran	2009-2010
Fiche 37	Infection par ver dans une centrale nucléaire – Slammer	USA	2003
Fiche 38	Arrêt d'urgence d'un réacteur nucléaire	USA	2008

INCIDENTS ANALYSÉS

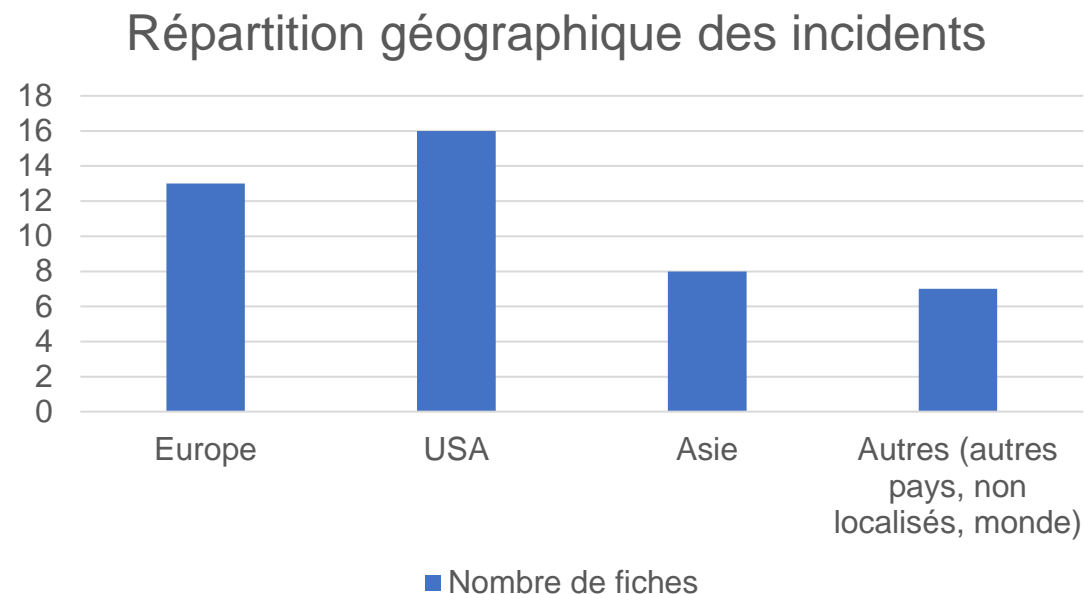
Autre

Fiche 39	Détournement d'un drone de reconnaissance	Iran	2011
Fiche 40	Attaque de terminaux de points de vente – BlackPOS	USA	2013
Fiche 41	Attaque sur une pompe à insuline	Monde	2011
Fiche 42	Récolte d'informations sur des systèmes médicaux – Orangeworm	Monde	2018
Fiche 43	Prise de contrôle des sirènes d'urgence – Dallas	USA	2017
Fiche 44	Blocage du système de contrôle d'accès aux chambres	Autriche	2017

ANALYSE DES INCIDENTS

L'analyse de la répartition géographique des incidents (hors rançongiciels) dévoile plusieurs éléments sur la situation économique et réglementaire des pays. On remarque en effet 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 et par une réglementation obligeant les entreprises à signaler certains incidents.



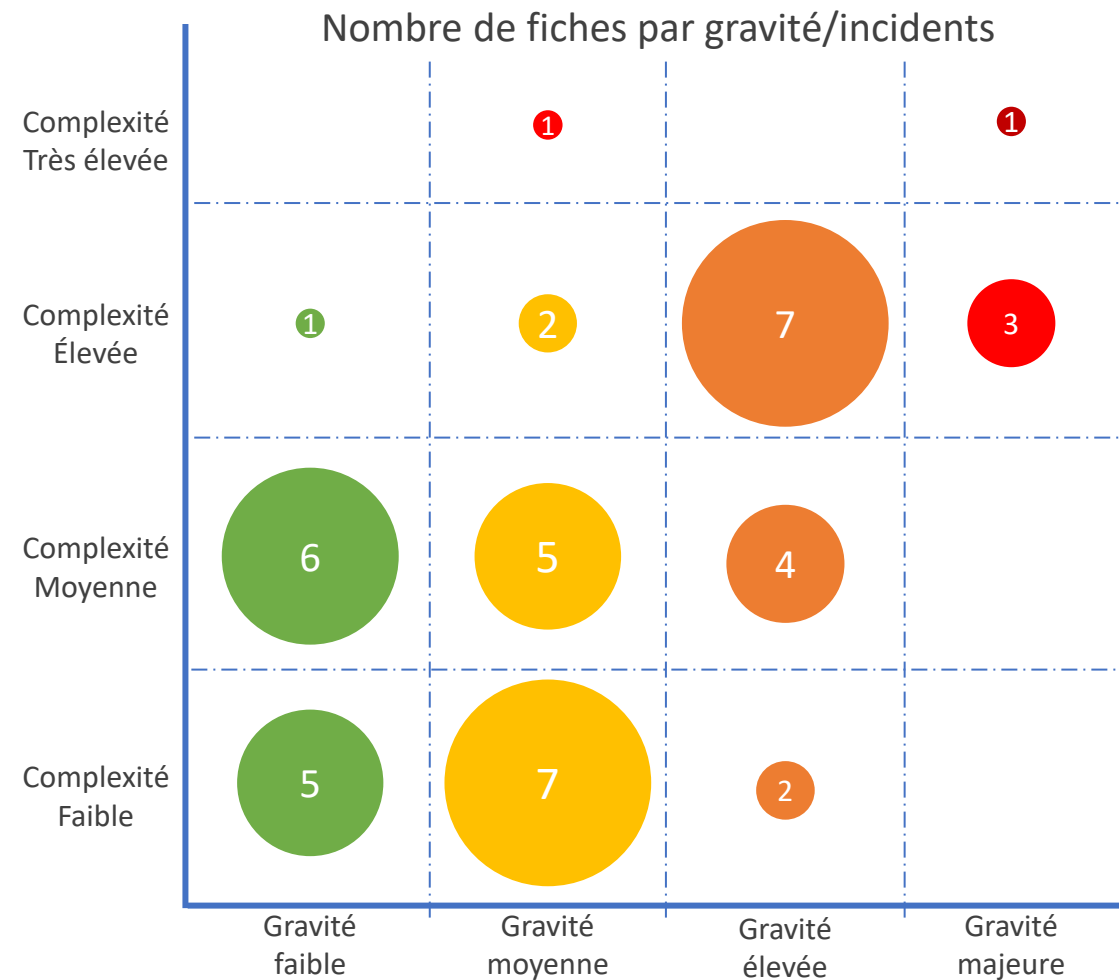
ANALYSE DES INCIDENTS

Le GT a référencé des attaques sur des 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.



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.

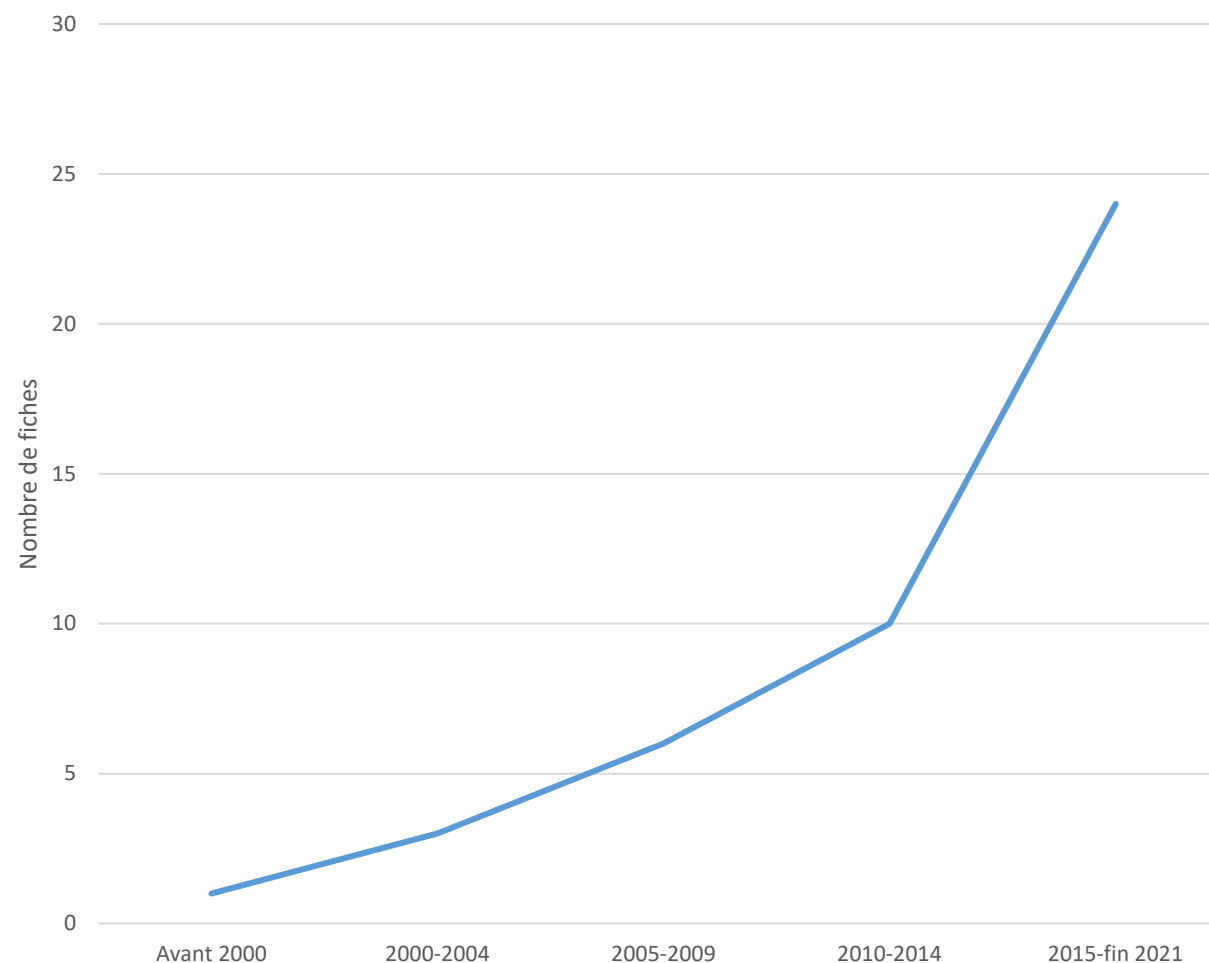
Il est à noter que dans le périmètre de ce travail, les attaques ayant eu un impact sur les systèmes de production ou les systèmes d'information industriels (ou réseau proche) sont en **constante augmentation**. Plusieurs facteurs peuvent expliquer cette tendance qui se confirme d'année en année :

- la connectivité numérique accrue des systèmes industriels (convergence IT/OT, produit sur étagère...) ;
- le manque de maturité des intervenants ;
- la professionnalisation des attaques par rançongiciel.

De plus, il transparaît de l'analyse de ces différentes attaques que cette transformation numérique des systèmes industriels n'a pas toujours été accompagnée par des **mesures de sécurité adéquates**.

Les mesures possibles sont notamment détaillées par le *Panorama des référentiels*, publié en 2014 et mis à jour en 2018 ainsi que le *Guide cybersécurité des systèmes industriels*, publié en 2021.

Répartition temporelle des fiches incidents



ANALYSE DES INCIDENTS

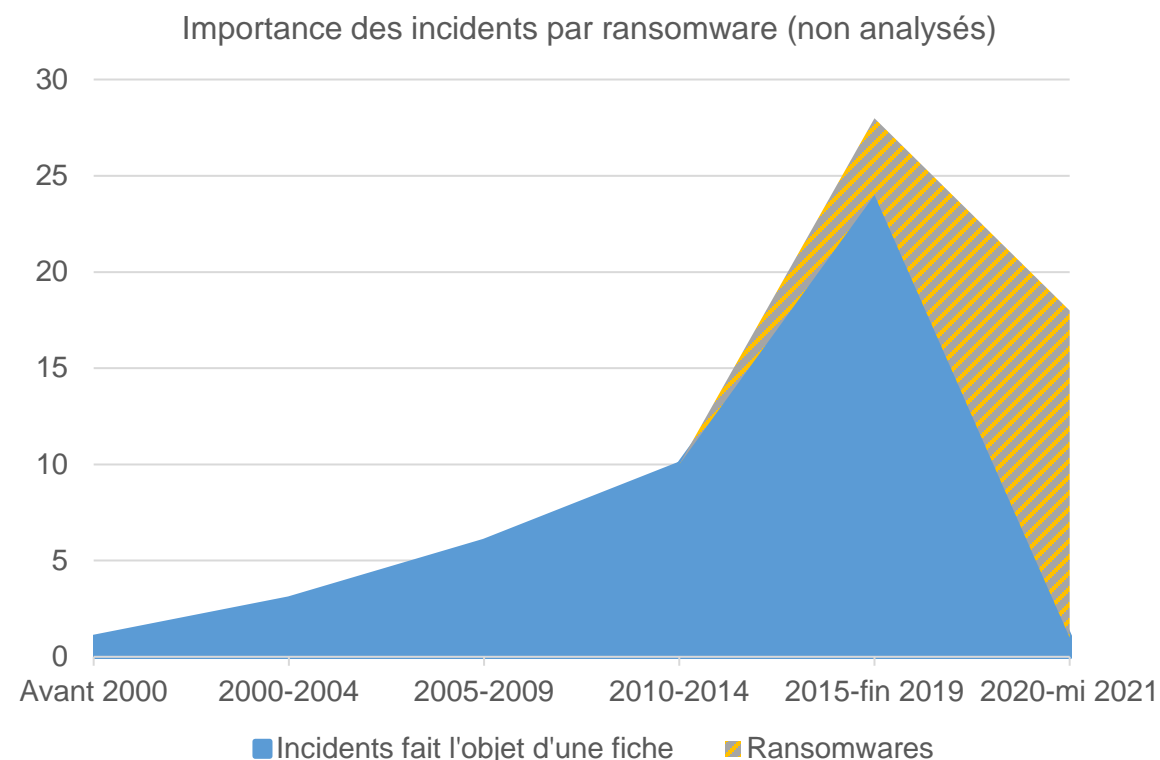
Dans son exercice de veille sur les incidents de sécurité, le GT Cybersécurité des systèmes industriels a identifié de nombreux incidents causés par des rançongiciels. Comme expliqué dans la démarche adoptée pour la rédaction de ce document, il a été décidé de ne pas traiter une fiche incident par rançongiciel.

Cependant, une analyse quantitative a été effectuée qui est en phase avec les différentes tendances observées concernant le niveau de menace.

Il est possible de noter la croissance du nombre de rançongiciels au cours des dernières années et notamment depuis Wannacry et NotPetya.

Cette croissance témoigne de la prolifération et professionnalisation de groupes cybercriminels (RaaS – Ransomware as a Service) pour lesquels une attaque par rançongiciel représente un avantage financier et lucratif non négligeable.

Cette observation, quoique basée sur un périmètre restreint (uniquement les incidents dont les membres du GT ont eu écho au travers de sources publiques) est en phase avec celles de l'ANSSI ¹.



ANALYSE DES INCIDENTS

Quid des rançongiciels ?

Le travail du GT étant basé sur des sources publiques, l'analyse est effectuée à partir de ces sources, qui la plupart du temps, fournissent des informations limitées. Ceci est notamment vrai pour le cas des incidents par rançongiciels.

En effet, dans ce type d'incident, les sources publiques évoquent l'impact opérationnel qui se traduit par une interruption ou perturbation des opérations industrielles. Le chemin de compromission n'étant pas toujours explicité, il n'a pas été possible d'identifier si les rançongiciels **ciblaient les systèmes industriels** ou si **ces derniers sont des cibles collatérales d'une attaque visant les systèmes d'information bureautiques**.

En effet, de nombreuses attaques par rançongiciel ayant pour cible les systèmes bureautiques ont pour conséquence des impacts sur les productions industrielles avec notamment une :

- Impossibilité de planifier les productions ;
- Impossibilité de faire un suivi de facturation ;
- Déconnexion des systèmes industriels par précaution.

Ceci témoigne de l'interconnexion entre les systèmes bureautiques et industriels, mais également de l'importance de cette interconnexion et de l'urgence à la sécuriser.

ANALYSE DES INCIDENTS

Quid des rançongiciels ?

Le GT a analysé quelques incidents causés par des rançongiciels. Certains incidents ont fait l'objet d'une fiche dédiée comme par exemple Wannacry et NotPetya.

Les incidents qui n'ont pas fait l'objet de fiche incident ont été répertoriés en fonction du scénario de compromission et du secteur touché.

Il est à noter que la majorité de ces incidents ont eu lieu en France. Ceci n'est pas dû au fait que la France soit particulièrement ciblée, mais plutôt que la presse locale relate plus les incidents locaux que les attaques par rançongiciel subies par des sites industriels dans d'autres pays. Il est bien évident que les attaques par rançongiciel sont mondialisées.

	Transport	Industrie			Chimie
Rançongiciel touchant le SI bureautique et impactant indirectement la production industrielle	RavnAir	X-Fab	Usines américaines de chimie (Hexion, Momenive)	Pilz	Usine à gaz naturel aux USA
		Fleury-Michon		Fabricant de puces Tower	
		Mont-Blanc*	Asco*	Picanol*	
Rançongiciel impactant directement le SI industriel	Port aux USA – Ryuk			Norsk Hydro	
				Honda	
				Ouest-France	

Répartition des incidents par rançongiciel identifiés par le GT en fonction du secteur et du scénario de compromission

*Les sources n'ont pas permis une catégorisation claire

SYNTHÈSE

Les incidents sont en nombre croissant, avec plusieurs causes :

La généralisation de l'utilisation 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 internes et externes) et **physiques** (circulation des personnes, clés USB, PC portables...) aux interconnexions entre le SI industriel et le SI bureautique, et au sein du SI industriel (procédure d'isolement en cas d'alerte, authentification forte, etc.).

La sensibilisation des acteurs intervenant sur les systèmes industriels quant aux risques liés à la sécurité informatique.

La surveillance des flux afin de détecter des attaques : les intrusions les plus complexes étant précédées de phases de reconnaissance, la maîtrise par l'exploitant des flux légitimes sur son réseau industriel doit permettre de repérer les activités anormales.

L'ensemble de ces mesures doit être **maintenu dans le temps** grâce à des processus et une organisation de la sécurité des systèmes d'information industriels.



QUELLES TENDANCES POUR LES ANNÉES À VENIR?



L'évolution croissante des incidents reflète en partie **l'augmentation du niveau de menace et de la vulnérabilité** des SI industriels.

La professionnalisation des groupes cybercriminels, la « démocratisation » des malwares (Ransomware as a Service) ainsi que l'intégration de technologies « bureautiques » en milieu « industriel » (automate connecté au cloud, par exemple) sont des preuves de cette augmentation de la menace.

Avec **l'émergence de l'industrie 4.0**, l'introduction massive des objets connectés au niveau terrain ainsi que l'ouverture sur le *Cloud* risquent **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**, qui sont, pour la plupart d'entre elles, constituées de systèmes industriels se renforcent et exigent un niveau minimum de cybersécurité pour les infrastructures critiques et de services essentiels. En effet, **les systèmes industriels sont des cibles de premier choix** pour la déstabilisation d'un état au regard des impacts que peuvent engendrer les attaques.

Enfin, les industriels (vendeurs et intégrateurs) commencent à s'intéresser à la cybersécurité, ce qui témoigne d'une prise de conscience du marché (clients finaux). Cet intérêt transparaît au travers de **l'intégration de la sécurité dans leurs produits** (certifications de produits) ou **proposition de services de sécurité** (conseil, veille, etc.).



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 plus graves ne surviennent.

Le Clusif espère y contribuer *via* ce jeu de « fiches incidents ».



FICHES INCIDENTS



- Impact

Blocage des opérations ou passage en mode dégradé

- Scénario d'incident

Compromission du système d'information bureautique impactant la production industrielle. Dans certains cas, le rançongiciel se propage également sur le système industriel.

- Vulnérabilité

Absence des règles de base d'hygiène informatique

ATTAQUES PAR RANÇONGICIEL

Gravité de l'attaque

Élevée

Motivation de l'attaquant

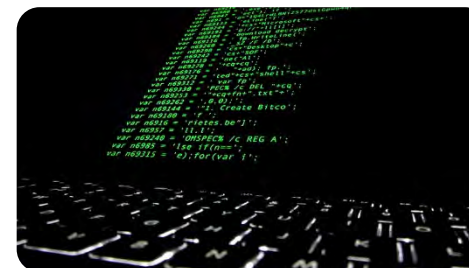
Financière

Complexité de l'attaque

Élevée

Déroulement de l'attaque

- Les attaques par rançongiciels impactant les systèmes industriels peuvent être de deux types :
 - Rançongiciel se propageant uniquement sur le périmètre bureautique ;
 - Rançongiciel se propageant sur les systèmes industriels.
- Dans les deux cas, la capacité de production des sites industriels est impactée à cause de l'incapacité du système à poursuivre la production (dans le cas d'attaques se propageant sur les SI), à superviser la production ou à conduire les actions associées de facturation, réservation, etc. (dans le cas d'attaques se limitant aux SI bureautiques).
- Selon le rançongiciel utilisé par les acteurs malveillants, différentes vulnérabilités sont exploitées.



Moyens mis en œuvre

- Ryuk, LockerGoga, etc.

Enseignements à tirer, préconisations et contre-mesures

- L'attaque d'un système bureautique peut induire une production dégradée. Ainsi, la sécurité des systèmes industriels ne peut être réalisée sans un traitement global de l'ensemble des systèmes d'information. Il reste cependant important de se protéger d'une compromission du système industriel étant donné les impacts potentiels sur la sûreté des hommes, de l'environnement et des biens.
- Plusieurs mesures de sécurité peuvent être entreprises pour réduire la probabilité de telle attaque et réduire leur impact. Parmi ces mesures, il est possible de noter :
 - Le **cloisonnement** des systèmes d'information (bureautique et industriel) ;
 - L'application de **politiques de maintien en condition de sécurité** ;
 - Le **durcissement** des systèmes (installation d'antivirus, EDR, politiques de contrôles d'accès, etc.), notamment l'Active Directory ;
 - La préparation de la **réponse à l'incident** via la génération de **sauvegardes**, de **procédures de gestion de crise** et les tester.
- Il existe plusieurs référentiels de sécurité permettant d'identifier les mécanismes à déployer. Il est recommandé de parcourir le panorama des référentiels du GT pour identifier les mesures à appliquer.

Tout secteur

Monde

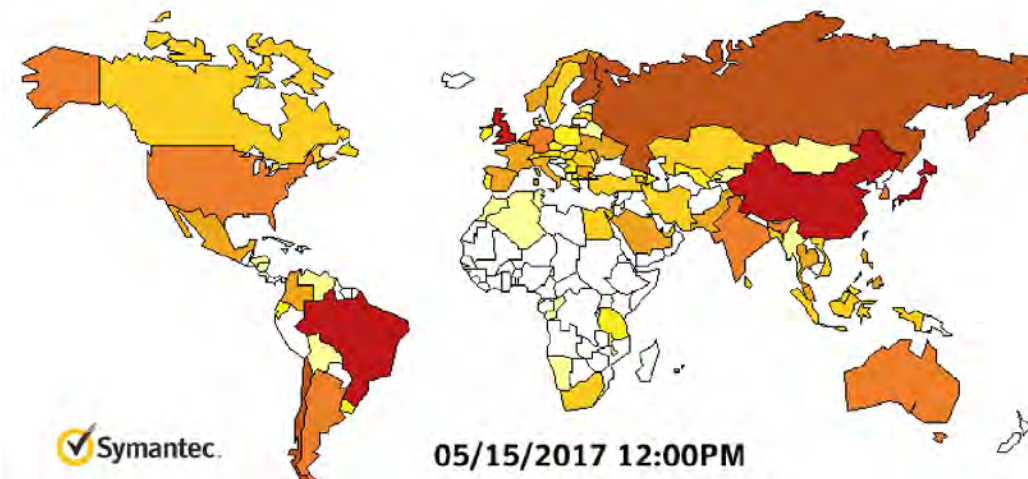
RANÇONNAGE DES SERVICES DE SANTÉ BRITANNIQUES – WANNACRY

2017

Santé

Royaume-Uni

Fiche 1



• Impact

Cyberattaque **mondiale** entraînant l'annulation de **milliers de rendez-vous et d'interventions médicales** (81 des 236 centres de santé impactés)

• Scénario d'incident

Attaque mondiale par rançongiciel

• Vulnérabilité

Utilisation de systèmes obsolètes
Non-déploiement de correctifs



RANÇONNAGE DES SERVICES DE SANTÉ BRITANNIQUES – WANNACRY



Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Attaque indifférenciée

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Le vendredi 12 mai 2017, une attaque mondiale par rançongiciel a contaminé plus de 200 000 ordinateurs dans près de 150 pays.
- WannaCry est composé de deux parties :
 - Un module Worm (ver) utilisant des vulnérabilités du serveur SMB de Microsoft Windows (CVE-2017-0144 et CVE-2017-0145) pour s'autopropager ;
 - Un module rançongiciel pour gérer les activités d'extorsion de rançon.
- Ce piratage a entraîné l'annulation de plus de 19 000 rendez-vous, ce qui a coûté 20 millions de livres sterling au NHS entre le 12 et le 19 mai et 72 millions de livres sterling pour le nettoyage et la mise à niveau de son système informatique.



Moyens mis en œuvre

- Faibles de sécurité de Microsoft Windows faisant partie d'un ensemble d'outils de piratage révélés par un groupe prénommé « The Shadowbrokers »
- Malware à large spectre d'utilisation intégrant Eternalblue (accès initial) et Doublepulsar (backdoor et persistance)
- Campagne ciblée d'emails infectés (*spear phishing*)



Enseignements à tirer, préconisations 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 limiter l'impact opérationnel d'une attaque par rançongiciel.
- Les mesures suivantes auraient permis de s'en prémunir :
 - Surveillance du comportement et des ressources utilisées par les équipements et des échanges autorisés** entre les équipements (installation d'un équipement de surveillance de la cartographie et d'analyse comportementale du système type NIDS) ;
 - Mise en place d'un mécanisme de liste blanche** au niveau des applications utilisables par les stations et serveurs (voire la mise en place d'un mécanisme de solidification des postes) ;
 - Blocage** des macros Office et sensibilisation des employés à la sécurité ;
 - Cloisonnement** plus important des réseaux (utilisation de diode par exemple) ;
 - Déploiement régulier des **misés à jour de sécurité** sur les postes et serveurs et mise en place d'une procédure de **gestion de l'obsolescence**.

ATTAQUE D'AMPLEUR MONDIALE – NOTPETYA

2017

Multi-sectoriel

Monde

Fiche 2



• Impact

Plus de 10 milliards d'euros de pertes d'exploitation chez des dizaines d'industriels : transporteurs, construction, industrie pharmaceutique, pétrolière...

• Scénario d'incident

Malware exploitant la faille EternalBlue (comme Wannacry), distribué *via* une mise à jour corrompue d'un logiciel et chiffrant irrémédiablement les disques durs.

• Vulnérabilités

Postes obsolètes (XP) ou non patchés, manque de cloisonnement

ATTAQUE D'AMPLEUR MONDIALE – NOTPETYA



Gravité de l'attaque

Majeure

Motivation de l'attaquant

Stratégique inter-États

Complexité de l'attaque

Élevée



Déroulement de l'attaque

- La société ukrainienne Intellect Service, éditrice du logiciel de comptabilité M.E.Doc utilisé pour les déclarations fiscales en Ukraine, est piraté.
- Les attaquants modifient le logiciel M.E.Doc en y intégrant une backdoor. Des mises à jour frauduleuses sont créées, intégrant l'exploit Eternalblue, Mimikatz, et un mécanisme de chiffrement non réversible des disques.
- Le 27 juin, le site web servant les mises à jour est corrompu de telle sorte qu'il redirige les connexions vers un serveur servant les mises à jours corrompues.
- Les mises à jour corrompent des milliers de postes, en Ukraine, mais aussi dans d'autres pays (sociétés commerçant avec l'Ukraine).
- Des réseaux entiers tombent suite à une corruption initiale, par exemple tous les serveurs Active Directory de Maersk (sauf un, déconnecté).



Moyens mis en œuvre

- Infiltration chez l'éditeur du logiciel M.E.Doc, corruption d'une mise à jour
- Combinaison EternalBlue et Mimikatz, une attaque de type « pass-the-hash »
- Camouflage en rançongiciel
- Diffusion simultanée via M.E.Doc et *phishing* par email



Enseignements à tirer, préconisations et contre-mesures

- La vulnérabilité exploitée par EternalBlue était connue et le risque présent car le monde avait subi Wannacry. Cependant, plusieurs systèmes n'avaient pas mis en place des mesures de protection ou de détection de cette menace.
- Concernant les systèmes d'exploitation ne pouvant pas tous être à jour (mise à jour de sécurité) pour des raisons opérationnelles, il faut s'assurer de la mise en place de mesures compensatoires pour éviter une exposition à des menaces pouvant exploiter les vulnérabilités.
- Les mesures suivantes auraient permis d'empêcher l'attaque ou d'en réduire l'impact :
 - Les **mises à jour** doivent être testées avant d'être déployées en production ;
 - Un **plan de reprise d'activité** (PRA) doit être prévu pour les éléments les plus critiques du SI, notamment les serveurs Active Directory ;
 - Des stratégies de **cyberrésilience** doivent être mises en œuvre (par exemple, isolation de réseaux en cas d'alerte, organisation de cellules de crises) ;
 - Le **cloisonnement** réseau permet de limiter la propagation des infections ;
 - Les **menaces provenant de l'écosystème** (fournisseurs, partenaires, clients...) doivent être analysées, comme le préconise l'ANSSI (via une analyse de risque telle qu'EBIOS Risk Manager, par exemple).

INTERRUPTION DE PRODUCTION D'ÉLECTRICITÉ

2015

Énergie

Ouessant, France

Fiche 3



- **Impact**

Arrêt de la 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

Gravité de l'attaque

Faible

Motivation de l'attaquant

Financière

Complexité de l'attaque

Faible

Déroulement de l'attaque

- Les attaquants ont **chiffré le serveur** permettant la connexion satellitaire avec l'unité de pilotage de l'hydrolienne.
- **Une rançon de 4 000 \$** à payer par PayPal ou par bitcoin afin de rétablir la connexion a été demandée.
- 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

Enseignements à tirer, préconisations 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 ;
 - **Maîtrise de 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.

COUPURE GÉNÉRALE D'ÉLECTRICITÉ – BLACKENERGY



2015

Énergie

Ivano-Frankivsk, Ukraine

Fiche 4



- **Impact**

80 000 foyers ukrainiens privés d'électricité, interruption d'une durée de 3 à 6 heures

- **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



Gravité de l'attaque

Élevée

Motivation de l'attaquant

Stratégique inter-États

Complexité de l'attaque

Élevée



Déroulement de l'attaque

- Une vague de *phishing* cible trois 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 de très fortes compétences techniques
- Malware (BlackEnergy)
- Campagne ciblée d'emails infectés (*spear phishing*)



Enseignements à tirer, préconisations 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 (deux 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 firmwares).

EXFILTRATION DE DONNÉES DE COMPAGNIES D'ÉNERGIE – HAVEX



2013-2014

Énergie

Europe, USA

Fiche 5



- **Impact**

Vol de données

- **Scénario d'incident**

Compromission 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



Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Espionnage

Complexité de l'attaque

Élevée



Déroulement de l'attaque

Un groupe de hackers dénommé Dragonfly a utilisé trois stratégies différentes pour infecter les réseaux informatiques de plus de 1 000 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 malveillants **chargés d'infecter les visiteurs par des chevaux de Troie** ;
- Infection **des mises à jour de logiciels SCADA de trois 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)



Enseignements à tirer, préconisations 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 configuration** des ordinateurs (*whitelisting*) qui pourront détecter l'installation de portes dérobées ;
 - **Mise en place d'un processus de test des mises à jour logicielles.**



- Impact

Déconnexion des accès distants des 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



Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Espionnage

Complexité de l'attaque

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



Enseignements à tirer, préconisations et contre-mesures

- Les entreprises développant des logiciels pour SI industriel doivent **protéger les environnements de développement** et s'assurer qu'ils 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.**

ARRÊT AUTOMATIQUE DE PROCESSUS INDUSTRIEL – TRITON

2017

Énergie

Arabie saoudite

Fiche 7



- **Impact**

Déclenchement du système instrumenté de sûreté (SIS) induisant l'arrêt automatique du processus industriel.

- **Scénario d'incident**

Compromission des contrôleurs SIS Triconex (Schneider Electric)

- **Vulnérabilité**

Vulnérabilité dans le firmware version 10.3 de Triconex

ARRÊT AUTOMATIQUE DE PROCESSUS INDUSTRIEL – TRITON



Gravité de l'attaque

Élevée

Motivation de l'attaquant
Stratégique inter-États

Complexité de l'attaque

Élevée



Déroulement de l'attaque

- L'attaque est basée sur un logiciel malveillant conçu pour les systèmes Triconex (SIS) de Schneider Electric et déployé contre au moins une victime au Moyen-Orient.
- L'attaquant a pu accéder à distance à un poste de travail technique du SIS, puis a déployé le malware afin de reprogrammer les contrôleurs SIS.
- Pendant l'incident, certains contrôleurs SIS ont déclenché leur système de sécurité, avec pour conséquence l'arrêt automatique du processus industriel et l'alerte du responsable des équipements. Les contrôleurs SIS ont déclenché la procédure d'arrêt d'urgence à cause de l'échec de validation d'un test de redondance entre unités physiques distinctes.
- Il est probable que l'attaquant ait stoppé accidentellement les opérations alors qu'il se préparait à causer des dégâts physiques sur l'infrastructure infiltrée.



Moyens mis en œuvre

- Un groupe d'individus expérimentés ayant une bonne connaissance des systèmes industriels, des contrôleurs Triconex et de très fortes compétences techniques
- Malware (Triton/Trisis/Hatman) pouvant communiquer avec les automates et incluant plusieurs fonctionnalités (il peut être considéré comme un framework)



Enseignements à tirer, préconisations et contre-mesures

- Cette attaque montre que des groupes malveillants commencent à prendre pour cible les systèmes de sûreté qui sont mis en place pour prémunir des dégâts sur la sécurité physique des personnes et de l'environnement.
- Les mesures suivantes auraient permis d'éviter l'attaque :
 - Déploiement des SIS sur des **réseaux isolés** du SI industriel ou avec un **filtrage très strict** (autorisation uniquement de flux de lecture) ;
 - **Durcissement** des postes et serveurs devant interagir avec les systèmes de sûreté (mise en place d'un contrôle d'accès, mécanisme de liste blanche au niveau des applications utilisables, surveillance, etc.) ;
 - Configuration des stations opérateur pour **afficher une alarme** lorsque la clé Tricon est en « mode programme ».

Note : Les rapports signalent que l'attaque détectée serait vraisemblablement une **expérimentation** visant à développer le malware pour lancer des attaques ultérieures.



- **Impact**

Arrêt des turbines, envoi d'informations erronées aux opérateurs

- **Scénario d'incident**

Intrusion physique et installation d'un ordinateur sur le réseau

- **Vulnérabilité**

Faible sécurité physique, absence de cloisonnement au sein du réseau industriel

PRISE DE CONTRÔLE D'ÉOLIENNE

Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Recherche

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Des chercheurs ont croché une serrure protégeant l'accès à une éolienne.
- Ils ont ensuite installé un Raspberry relié à une antenne Wi-Fi au sein du réseau interne à l'éolienne.
- En prenant le contrôle distant du Raspberry, les chercheurs ont réussi à découvrir les adresses IP de l'ensemble des turbines du parc éolien.
- Ils ont alors eu accès aux turbines et pu envoyer des commandes d'arrêt d'urgence. Ces arrêts peuvent endommager les turbines.



Moyens mis en œuvre

- Raspberry avec antenne Wi-Fi
- Outils développés pour faire une attaque de l'Homme du milieu (*man in the middle*)



Enseignements à tirer, préconisations et contre-mesures

- Malgré le fait que le parc éolien n'était pas connecté à Internet, le système d'information n'était pas cloisonné en différentes zones. La sécurité du système d'information reposait donc sur la sécurité physique d'une turbine.
- Les mesures suivantes auraient permis de s'en prémunir :
 - Étude de la **sécurité physique du système d'information** et mise en place des mesures nécessaires ;
 - **Cloisonnement** du système d'information en différentes zones de criticité et interdiction des communications non nécessaires (en fonction de la criticité des ressources, un cloisonnement et filtrage de PVLAN peut s'avérer nécessaire) ;
 - Mise en place d'un **mécanisme d'authentification** du système de contrôle d'une turbine.

DÉNI DE SERVICE SUR UN CHAUFFAGE PUBLIC - MIRAI

2016

Énergie

Lappeenranta, Finlande

Fiche 9



- **Impact**

Arrêt du système de chauffage public d'un ensemble d'habitations

- **Scénario d'incident**

Attaque par déni de service lancée par un réseau de machines compromises

- **Vulnérabilité**

Système de chauffage exposé sur Internet

DÉNI DE SERVICE SUR UN CHAUFFAGE PUBLIC - MIRAI

Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Attaque indifférenciée

Complexité de l'attaque

Faible



Déroulement de l'attaque

- Fin octobre 2016, une attaque par déni de service est lancée sur un système de chauffage public dans une ville de 60 000 habitants en Finlande.
- L'attaquant a utilisé un réseau de machines compromises (botnet) pour lancer cette attaque.
- La multitude de requêtes a eu pour conséquence le redémarrage répétitif du système rendant indisponible le chauffage ainsi que l'eau chaude aux bâtiments.
- La compagnie gérant le système est passée en mode manuel et mis en place un pare-feu en coupure.
- L'attaque prit fin le 3 novembre.



Moyens mis en œuvre

- Réseau de machines zombies (botnet Mirai)



Enseignements à tirer, préconisations et contre-mesures

- Les systèmes industriels ne doivent pas être exposés sur Internet sans protection. Les besoins de supervision à distance des systèmes doivent être encadrés.
- La mise en place d'un **pare-feu n'autorisant que les flux légitimes** (intégrant de préférence un système anti-DDoS) aurait permis de se prémunir d'une telle attaque.

ATTAQUE SUR UN RÉSEAU ÉOLIEN ET SOLAIRE

2019

Énergie

Utah, USA

Fiche 10



- **Impact**

Pertes de connexion pendant plusieurs intervalles de 5 minutes durant 12 heures entre une **douzaine d'installations de production d'énergie éolienne et solaire** et le centre de contrôle du réseau de l'entreprise

- **Scénario d'incident**

Exploitation d'une vulnérabilité connue sur des pare-feu non patchés provoquant un déni de service des équipements

- **Vulnérabilité**

Absence de maintien en condition de sécurité des équipements fortement exposés

ATTAQUE SUR UN RÉSEAU ÉOLIEN ET SOLAIRE



Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Attaque indifférenciée

Complexité de l'attaque

Faible



Déroulement de l'attaque

- Le 5 mars 2019, un fournisseur d'énergie renouvelable (sPower) basé dans l'Utah a subi une attaque informatique de déni de service sur des **pare-feu non patchés** Cisco en exploitant une **vulnérabilité connue** de l'équipement.
- Ce déni de service a engendré des **pertes de connexion** de supervision pendant plusieurs intervalles de cinq minutes entre de 9 h à 19 h. Ces pertes de connexion concernaient une **douzaine d'installations de production** d'énergie éolienne et solaire totalisant **500 MW** et situées en **Californie, en Utah et au Wyoming**.
- L'incident n'a, fort heureusement, **pas affecté les systèmes de contrôle les plus critiques** de l'entreprise et n'a **pas eu d'incidence sur sa production d'énergie**.



Moyens mis en œuvre

- Réseau de machines zombies (*botnets*) effectuant des campagnes de balayage à la recherche d'équipements non patchés et exposés sur Internet



Enseignements à tirer, préconisations et contre-mesures

- Un processus de **gestion des vulnérabilités** doit être mis en œuvre afin de rechercher les correctifs disponibles pour corriger ces vulnérabilités et de **déployer ces correctifs** en commençant par les plus importants (apport en sécurité, simplicité de déploiement, etc.).
- Les vulnérabilités qui ne peuvent pas être corrigées, soit par manque de correctifs, soit parce que le correctif n'a pas pu être appliqué en raison de contraintes opérationnelles, doivent être recensées. Un suivi spécifique doit être mis en œuvre et des **mesures palliatives** doivent être appliquées pour diminuer l'exposition due à ces vulnérabilités.
- Les correctifs de sécurité doivent être appliqués en priorité sur **les équipements les plus exposés** (stations d'ingénierie, consoles de programmation, pare-feu, VPN, etc.).

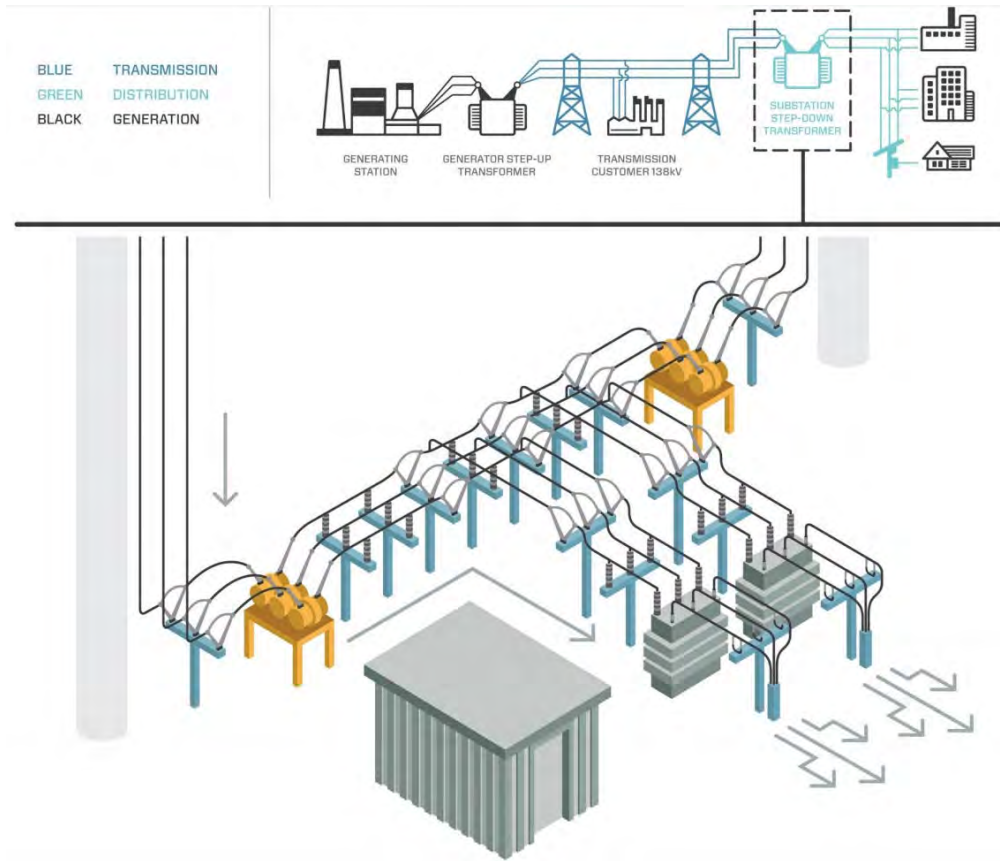
RUPTURE DU TRANSPORT D'ÉNERGIE ÉLECTRIQUE – CRASHOVERRIDE/INDUSTROYER

2016

Énergie

Kiev, Ukraine

Fiche 11



• Impact

Une partie des habitants de Kiev et de sa périphérie ont été privés d'électricité pendant environ une 1 heure

• Scénario d'incident

Déconnexion de la sous-station du réseau de transport électrique de Pivnichna (environs de Kiev) au moyen d'un malware spécialement développé pour ce domaine d'activité

• Vulnérabilité

Utilisation de protocoles de communication industriels légitimes **peu sécurisés**

RUPTURE DU TRANSPORT D'ÉNERGIE ÉLECTRIQUE – CRASHOVERRIDE/INDUSTROYER



Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Stratégique inter-États

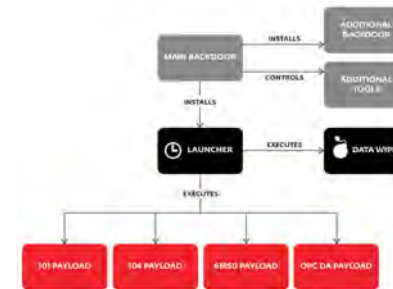
Complexité de l'attaque

Très élevée



Déroulement de l'attaque

- Une campagne de phishing lancée en juin 2016, ciblant des organisations gouvernementales, a permis l'accès initial au système IT d'une station électrique.
- Durant plusieurs mois, les attaquants analysent le fonctionnement du système ainsi que celui des équipements liés au contrôle de l'infrastructure d'alimentation en énergie.
- Un malware modulaire, incluant quatre protocoles de communication industriels (IEC 60870-5-101, IEC 60870-5-104, IEC 61850 et OPC DA), est utilisé pour contrôler les équipements des sous-stations électriques. Un module pouvant désactiver les systèmes de protection des équipements était aussi inclus dans le malware.
- Le 17 décembre, le malware envoie des commandes d'arrêt directement aux équipements de production et effectue un déni de service sur les équipements de protection générant une rupture de la distribution d'énergie. Cependant, le module de désactivation des équipements de protection n'a pas fonctionné.



Moyens mis en œuvre

- Un groupe d'individus expérimentés ayant une bonne connaissance des systèmes industriels
- Développement d'un malware spécifique incluant des protocoles connus dans l'industrie énergétique



Enseignements à tirer, préconisations et contre-mesures

- Les utilisateurs des systèmes industriels doivent être sensibilisés à la cybersécurité (sensibilisation au phishing) et à la **détection de compromission sur le périmètre industriel** (amélioration de la détection de signaux faibles de compromission masqués ou considérés comme des incidents de production du système).
- Le renforcement du **plan de continuité d'activité** (inclure la conduite d'installation en mode dégradé) et l'exécution d'exercices de simulation.
- Les mesures suivantes auraient permis de s'en prémunir :
 - **Renforcement du cloisonnement** entre les réseaux IT et OT (utilisation de diode ou de NIPS permettant de les isoler préventivement lorsqu'un incident est détecté) ;
 - **Mise en place d'un mécanisme de liste blanche** au niveau des applications utilisables par les stations et serveurs de la partie OT (mécanisme de solidification des postes opérateurs et d'ingénierie) ;
 - **Surveillance de la liste des échanges autorisés** entre les périmètres industriels et IT (installation d'un équipement de surveillance d'analyse comportementale du réseau).

EXPLOSION D'UN PIPELINE

2008

Pétrole & Gaz

Turquie

Fiche 12

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

Gravité de l'attaque

Élevée

Motivation de l'attaquant

Stratégique inter-États

Complexité de l'attaque

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 (également 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 puis son explosion.
- Le centre de surveillance du pipeline a eu connaissance de l'explosion 40 minutes après qu'elle a 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



Enseignements à tirer, préconisations 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 13



- **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

Gravité de l'attaque

Élevée

Motivation de l'attaquant

Politiques

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Un employé de la compagnie disposant d'un compte privilégié a probablement cliqué sur un lien contenu dans un message SCAM (**phishing**).
- Le **virus Shamoon** s'est rapidement déployé sur l'ensemble du réseau **30 000 postes de travail, 2 000 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



Enseignements à tirer, préconisations et contre-mesures

- La **sensibilisation** des utilisateurs reste un point important à prendre en compte.
- Les réseaux à plat permettent aux malwares de se déployer très facilement.
- Les mesures suivantes auraient permis de s'en prémunir ou d'en limiter la portée :
 - Mise en place des **systèmes de détection d'intrusion** ;
 - Cloisonnement du réseau par niveau de sensibilité ;
 - **Sensibilisation** des employés à la sécurité ;
 - Mise en place d'un **plan de continuité d'activité** en spécifiant l'utilisation de matériel de rechange.

EXPLOSION D'UN GAZODUC

1982

Pétrole & Gaz

URSS

Fiche 14

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

Gravité de l'attaque

Élevée

Motivation de l'attaquant

Stratégique inter-États

Complexité de l'attaque

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



Enseignements à tirer, préconisations 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).

VOL DE CARBURANT EN STATION-SERVICE

2018

Pétrole & Gaz

Israël

Fiche 15

Preuve de concept

- **Impact**

Arrêt de service, vol de carburant, potentielle fraude bancaire

- **Scénario d'incident**

Prise de contrôle du système de gestion des pompes des stations-service

- **Vulnérabilité**

Exposition des contrôleurs pompe directement sur Internet, nombreuses vulnérabilités connues



VOL DE CARBURANT EN STATION-SERVICE

Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Financière/Fraude

Complexité de l'attaque

Facile

Déroulement de l'attaque

- Des chercheurs en cybersécurité (Kaspersky, Azimuth) ont découvert des vulnérabilités dans le système qui contrôle des pompes de stations-service (SiteOMat Orpak) : après le plantage du contrôleur, l'écran affichait l'adresse IP publique de la station-service.
- La découverte des services exposés sur cette adresse a révélé la présence d'un service web protégé par le mot de passe par défaut, disponible dans le manuel utilisateur du constructeur.
- Ils ont ainsi pu pénétrer le système à distance et utiliser les vulnérabilités internes pour notamment changer les prix des carburants, mais aussi effacer toute trace des modifications.
- Grâce à Shodan¹, ils ont pu identifier plus de mille stations-service exposées. Le constructeur a corrigé ces vulnérabilités le mois suivant.

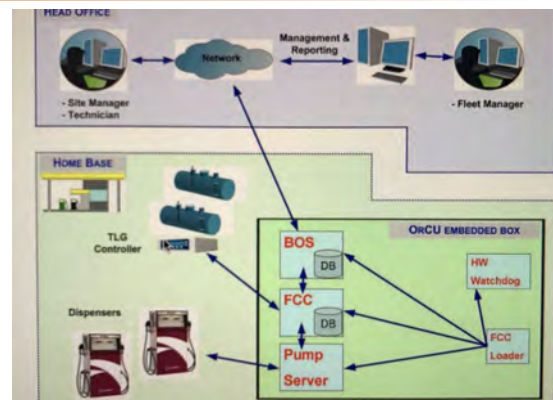


Schéma fonctionnel du SI Station-service

Moyens mis en œuvre

- Recherche des stations-service exposées sur Internet
- Utilisation de mot de passe par défaut
- Exploitation de failles dans les vulnérabilités existantes

Enseignements à tirer, préconisations et contre-mesures

- Il faut considérer que chaque système, chaque logiciel à risque est vulnérable à des attaques. Il faut donc mettre en place des mesures de défense en profondeur qui peuvent réduire le risque. L'évaluation de l'impact de la compromission du système permet de déterminer les bonnes mesures de sécurité à mettre en œuvre. L'identification des sous-systèmes accessibles (prix carburant, données bancaires), indique clairement que ce système pour station-service ne devrait pas être accessible directement depuis Internet.
- Les mesures suivantes auraient permis de s'en prémunir :
 - Cloisonnement** des systèmes de production de tout réseau (Internet ou réseau d'entreprise) via la mise en place d'un pare-feu ;
 - Modification** des mots de passe par défaut ;
 - Mise à jour** régulière des applications et systèmes.

¹ Moteur de recherche d'équipements connectés sur internet (shodan.io)

ATTAQUE D'UNE STATION D'ÉPURATION DES EAUX

2015

Eau/Assainissement

Lieu non communiqué

Fiche 16



- **Impact**

Perturbation du procédé de traitement des eaux usées

- **Scénario d'incident**

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

- **Vulnérabilité**

Faible dans une application en ligne reliée au système industriel

ATTAQUE D'UNE STATION D'ÉPURATION DES EAUX

Gravité de l'attaque

Faible

Motivation de l'attaquant

Fraude

Complexité de l'attaque

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 au travers d'**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



Enseignements à tirer, préconisations 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, échanges** entre les équipes IT et industrielles suite à un comportement suspect.

MISE HORS SERVICE D'UN SUPERVISEUR DE DÉRIVATION D'EAU

2007

Eau/Assainissement

Willows, USA

Fiche 17



- **Impact**

Déni de service du superviseur/5 000 \$ de dommages

- **Scénario d'incident**

Sabotage du superviseur par un employé licencié

- **Vulnérabilité**

Manque de suivi des droits d'accès des employés

MISE HORS SERVICE D'UN SUPERVISEUR DE DÉRIVATION D'EAU

Gravité de l'attaque

Faible

Motivation de l'attaquant

Vengeance

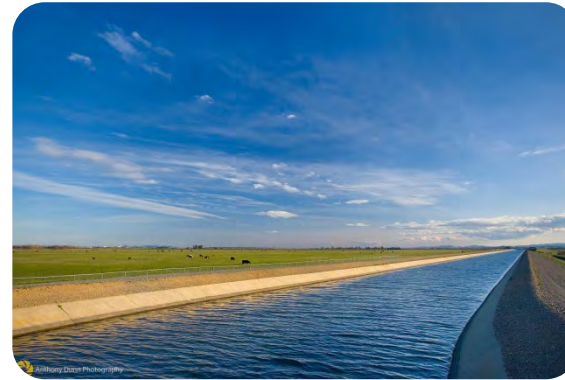
Complexité de l'attaque

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



Enseignements à tirer, préconisations 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.

DÉVERSEMENT D'EAUX USÉES

2000

Eau/Assainissement

Maroochy, Australie

Fiche 18



- **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

Gravité de l'attaque

Élevée

Motivation de l'attaquant

Vengeance

Complexité de l'attaque

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 candidaté pour un poste au sein de cette dernière.
- Sa demande d'emploi ayant été refusée, il a décidé de **se venger** des deux 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 avait 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



Enseignements à tirer, préconisations 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.

EMPOISONNEMENT DE L'EAU POTABLE

2013

Eau/Assainissement

Géorgie, USA

Fiche 19



- **Impact**

400 résidents privés d'eau

- **Scénario d'incident**

Modification des 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

Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Vengeance ?

Complexité de l'attaque

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 ne se trouvait à proximité de la station au moment de 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



Enseignements à tirer, préconisations 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 :
 - Renforcement des **contrôles d'accès physique** ;
 - **Surveillance** des zones à risque ;
 - **Révocation** des accès au départ d'un employé.

MINAGE DE CRYPTOMONNAIE MONERO

2018

Eau/assainissement

Europe (pays non connu)

Fiche 20



- **Impact**

Ralentissement du pilotage de l'exploitation

- **Scénario d'incident**

Logiciel de minage de cryptomonnaie détecté sur quatre IHM (interfaces homme-machine)

- **Vulnérabilité**

Système d'exploitation obsolète et absence de cloisonnement

MINAGE DE CRYPTOMONNAIE MONERO

Gravité de l'attaque

Faible

Motivation de l'attaquant

Financière

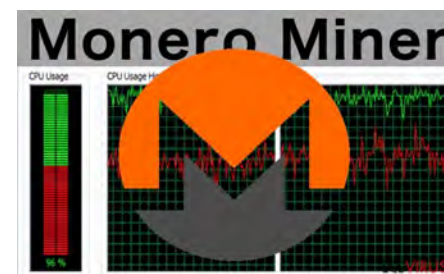
Complexité de l'attaque

Faible



Déroulement de l'attaque

- Une usine de traitement des eaux usées en Europe a été victime d'une attaque non ciblée par logiciel malveillant de minage de cryptomonnaie Monero.
- Le système d'information de l'usine présentait des connexions externes vers Internet pour la surveillance à distance de son fonctionnement.
- Le logiciel malveillant a infecté un premier serveur puis un total de quatre stations (utilisant Windows XP) en se propageant dans le réseau de façon furtive (« mode caché » actif). Il a ensuite ouvert une communication vers un serveur central qui coordonne l'extraction.
- Suite à un audit sur site, la connexion externe a été découverte et les investigations ont mené aux stations infectées. Cette découverte a expliqué la baisse de performance remarquée sur ces stations.



Moyens mis en œuvre

- Inclusion d'un des logiciels de minage de Monero (plusieurs logiciels de ce type circulent) dans un logiciel ou une extension de navigateur et mise à disposition *via* des sites web ou sites de partage n'effectuant aucune vérification sur le contenu mis à disposition



Enseignements à tirer, préconisations et contre-mesures

- Plusieurs mesures d'hygiène de base permettent de prévenir ce type d'infection, de la détecter ou de la rendre inoffensive :
 - **Cloisonnement du réseau industriel et contrôle des accès Internet** afin d'éviter des échanges directs entre les systèmes industriels et des zones de moindre confiance ;
 - **Blocage par liste blanche de processus** afin de prévenir l'exécution de code malveillant ;
 - **Mise à jour régulière** des systèmes d'exploitation et des applications ;
 - **Surveillance des flux entre le SI industriel et les zones de moindre confiance** ;
 - **Surveillance des processus** sur les stations et de leurs performances, qui aurait permis de détecter l'attaque et de réagir plus rapidement.
- À noter : de nombreux logiciels malveillants sont présents sur des réseaux industriels et sont inopérants du fait de l'absence de route vers Internet. Cependant, ils peuvent avoir un impact en provoquant des ralentissements sur un système hôte ne possédant pas beaucoup de ressources.
- Point positif : l'usine se fait auditer d'un point de vue cybersécurité. L'audit a permis de détecter l'infection.

MODIFICATION DES PARAMÈTRES D'UNE STATION DE TRAITEMENT D'EAU

2021

Eau/assainissement

Floride, USA

Fiche 21



- **Impact**

Modification de la concentration d'hydroxyde de sodium dans le processus de traitement des eaux

- **Scénario d'incident**

Prise de contrôle distante *via* Teamviewer sur une IHM et modification des paramétrages

- **Vulnérabilité**

Systèmes industriels accessibles directement depuis Internet et absence de mécanisme sécurisé de contrôle distants

MODIFICATION DES PARAMÈTRES D'UNE STATION DE TRAITEMENT D'EAU

Gravité de l'attaque
Faible

Motivation de l'attaquant
Attaque indifférenciée

Complexité de l'attaque
Faible



Déroulement de l'attaque

- Un attaquant a réussi à obtenir l'accès au réseau industriel d'une station de traitement des eaux d'une ville de Floride.
- L'attaquant a ensuite eu accès à une interface homme-machine permettant de contrôler la concentration d'hydroxyde de sodium utilisée par la station. Il a alors augmenté cette concentration, passant de 100 particules par million à 11 100 particules par million. À cette concentration, l'eau aurait pu être dangereuse pour chaque personne en contact avec celle-ci.
- Les opérateurs ont immédiatement remarqué cette modification et corrigé la concentration.
- Dans les rapports, il est indiqué que des mécanismes supplémentaires empêchant la contamination de l'eau ont bloqué les accès distants.



Moyens mis en œuvre

- Accès Teamviewer



Enseignements à tirer, préconisations et contre-mesures

- L'attaquant n'a pas cherché à cacher son action en empêchant les opérateurs de détecter la modification des concentrations. Il s'agirait d'une attaque opportuniste d'un acteur ayant réussi à récupérer des accès Teamviewer. Ces accès étaient ceux utilisés par le responsable pour accéder au système. Il est ainsi important de s'assurer du cloisonnement du réseau industriel et mettre en place des mécanismes sécurisés d'accès distants.
- Les mesures suivantes auraient permis d'empêcher cette attaque :
 - **Interdiction** des flux directs entre un réseau industriel et Internet ;
 - Mise en place d'un **mécanisme sécurisé d'accès distants** lorsqu'une prise en main distante est requise ;
 - **Sensibilisation** des opérateurs sur la nécessité d'authentifier les personnes souhaitant avoir accès aux postes (acquittement Teamviewer).

PRISE DE CONTRÔLE DE L'AIGUILLAGE D'UN TRAMWAY



2008

Transport

Lodz, Pologne

Fiche 22



- **Impact**

Dérailage de 4 tramways, 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



Gravité de l'attaque

Élevée

Motivation de l'attaquant

Ludique/Par challenge

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- À 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



Enseignements à tirer, préconisations 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

2015

Transport

Saint louis, USA

Fiche 23

Preuve de concept



- **Impact**

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

- **Scénario d'incident**

Prise de contrôle du véhicule par deux chercheurs

- **Vulnérabilité**

Réseau Wi-Fi 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



Gravité de l'attaque

Élevée

Motivation de l'attaquant

Sensibilisation

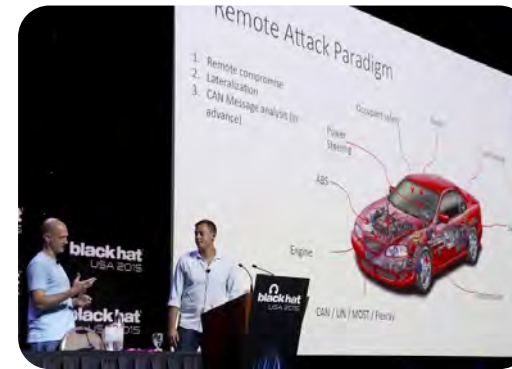
Complexité de l'attaque

Élevée



Déroulement de l'attaque

- Certaines voitures sont équipées d'une option permettant au conducteur de **contrôler la console de bord par Wi-Fi**. Les chercheurs ont réussi, en découvrant la clé Wi-Fi, 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



Enseignements à tirer, préconisations 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 Wi-Fi 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 :
 - **Utilisation d'un algorithme assurant une génération de clé non prédictible ;**
 - Mise en place d'un **mécanisme empêchant la mise à jour du Firmware** du contrôleur V850 par un code non signé ;
 - **Filtrage des communications** entre le contrôleur V850 et le CAN bus (ACL, pare-feu...).

PERTURBATION DES SYSTÈMES DE SIGNALISATION FERROVIAIRE – SOBIG & BLASTER



2003

Transport

États-Unis d'Amérique

Fiche 24



- **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) entraînant 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



Gravité de l'attaque
Élevée

Motivation de l'attaquant
Ludique

Complexité de l'attaque
Moyenne



Déroulement de l'attaque

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



Moyens mis en œuvre

- Le virus SoBig s'est propagé entre 2002 et 2003 en exploitant une faille de sécurité dans Windows, grâce à l'usage de courriels frauduleux
- Le virus Blaster s'est propagé en 2003, générant des attaques par déni de service
- Investissement financier faible



Enseignements à tirer, préconisations 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** (ex. : Office) pour limiter toute tentative de propagation de virus.

DÉMONSTRATEUR D'UNE ATTAQUE D'UNE STATION DE LAVAGE AUTOMOBILE

2017

Transport

USA

Fiche 25

Preuve de concept



- **Impact**

Dégradation du véhicule *via* les portes de la station de lavage auto ou les rouleaux. Risque de blessure de l'utilisateur en réussissant à contourner les capteurs de sécurité

- **Scénario d'incident**

PoC visant à s'introduire à distance dans le système pilotant la station de lavage automatique et en prenant le contrôle des différentes machines de l'équipement

- **Vulnérabilité**

Système connecté directement sur Internet, sans sécurité particulière, et avec un mot de passe faible

DÉMONSTRATEUR D'UNE ATTAQUE D'UNE STATION DE LAVAGE AUTOMOBILE



Gravité de l'attaque
Élevée

Motivation de l'attaquant
Sensibilisation

Complexité de l'attaque
Facile



Déroulement de l'attaque

- L'attaque a ciblé les systèmes de lavage auto connectés au réseau public pour la maintenance et le contrôle à distance du fabricant.
- L'intrusion à distance dans le système a été réalisée *via* l'utilisation d'un mot de passe trivial.
- À partir de ce moment, les attaquants ont obtenu le contrôle total du système, dont certains critiques, pouvant endommager les voitures ou blesser les utilisateurs.
- Les chercheurs ont envoyé des alertes successives au constructeur qui a finalement apporté des mesures correctives.



Moyens mis en œuvre

Même si le système d'exploitation utilisé était obsolète (Windows CE sur ARM), les attaquants ont simplement réussi à se connecter à distance, le système étant facilement accessible sur une adresse publique, en utilisant le mot de passe « 12345 ».



Enseignements à tirer, préconisations et contre-mesures

- Lors de la livraison des systèmes industriels, il est d'usage de mettre en place des mécanismes d'accès distants pour les besoins de maintenance. L'absence de sécurité sur ces mécanismes expose les systèmes. Il est nécessaire d'encadrer cette pratique.
- Les mesures suivantes auraient permis de s'en prémunir :
 - **Cloisonnement des équipements industriels** de tout réseau public. Si la connexion à distance est nécessaire, il est indispensable de mettre en place une architecture d'accès distant sécurisée ;
 - **Mise en place de mots de passe complexes** et régulièrement mis à jour ;
 - **Sélection des fournisseurs d'équipements industriels qui réalisent une veille de sécurité** et qui notifient leurs clients de la mise en service de solutions correctives

COMPROMISSION D'UN VÉHICULE

2017

Transport

Monde

Fiche 26

Preuve de concept



- **Impact**

Prise de contrôle de certains éléments d'un véhicule (frein, porte, signal, coffre, rétroviseurs, etc.)

- **Scénario d'incident**

Exploitation de **plusieurs vulnérabilités** impactant les modules du véhicule dans le cadre de travaux de recherche

- **Vulnérabilité**

Plusieurs 0Day ont été exploitées

COMPROMISSION D'UN VÉHICULE

Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Sensibilisation

Complexité de l'attaque

Très élevée



Déroulement de l'attaque

- En 2016, des chercheurs ont trouvé de nombreuses vulnérabilités sur plusieurs modules du véhicule (Tesla) permettant l'exécution de code à distance.
- Cette recherche a permis l'identification de 0Day qui ont été partagées avec le constructeur.
- Ce dernier a mis en place des mécanismes de sécurité dont un mécanisme de signature de code et a corrigé les vulnérabilités en 10 jours.
- De nouvelles recherches ont montré la capacité de détourner ces mécanismes de sécurité et ainsi de prendre le contrôle du système de freinage, des clignotants, etc.



Moyens mis en œuvre

- Plusieurs 0Day
- Plusieurs chercheurs ont travaillé sur le PoC



Enseignements à tirer, préconisations et contre-mesures

- Il est important de noter que le constructeur automobile a échangé avec les chercheurs, ce qui a permis l'identification des vulnérabilités et leur correction rapide.
- Tesla a mis en place depuis 2015 un programme de **bug-bounty** permettant la remontée de vulnérabilités découvertes.



- **Impact**

Ouverture d'un véhicule, accès à sa localisation ou usage du klaxon

- **Scénario d'incident**

Compromission de l'application mobile du véhicule et du serveur du vendeur pour s'attribuer des accès

- **Vulnérabilité**

Développement non sécurisé

OUVERTURE D'UN VÉHICULE

Gravité de l'attaque

Faible

Motivation de l'attaquant

Ludique/Par challenge

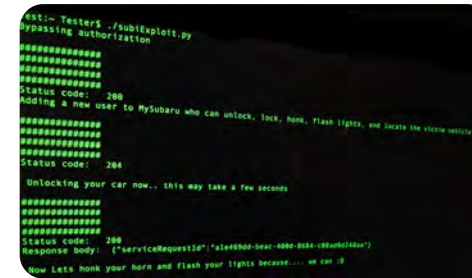
Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Un chercheur a réalisé des tests d'intrusion sur l'application mobile de contrôle d'un véhicule (Subaru).
- L'application communique avec un serveur (Starlink) qui présente des vulnérabilités (envoi de jetons d'authentification en clair sur le réseau, jetons qui n'expirent jamais, authentification ne reposant que sur le jeton seul, etc.). Le chercheur a ainsi trouvé huit vulnérabilités qui lui permettent de rajouter des utilisateurs à un compte détenteur d'un véhicule.
- Il est ainsi possible à un utilisateur de disposer d'un accès au véhicule, à sa localisation, à son historique d'utilisation ou même de klaxonner.



```
root@kali:~/Testers# ./subExploit.py
Bypassing authorization
#####
#####
#####
Status code: 200
Adding a new user to MySubaru who can unlock, lock, honk, flash lights, and locate the vehicle
#####
#####
#####
Status code: 200
Unlocking your car now... this may take a few seconds
#####
#####
#####
Status code: 200
Response body: {"serviceRequestId": "a1e1b0a0-0000-0000-0000-000000000000"}
Now Let's honk your horn and flash your lights because... we can :)
```



Moyens mis en œuvre

- Serveur web présentant des vulnérabilités de contrôle d'accès



Enseignements à tirer, préconisations et contre-mesures

- La sécurité d'un véhicule dépend également de la sécurité des mécanismes d'accès. Ainsi, l'utilisation d'application présentant des vulnérabilités permettrait à un attaquant de compromettre le véhicule.
- Les mesures suivantes auraient permis d'éviter cette compromission :
 - Application des **bonnes pratiques de développement**, notamment pour le développement d'application web et mobiles (utilisation d'OWASP par exemple) ;
 - Mise en place d'une **procédure de développement sécurisé** ;
 - **Conduite d'audits techniques** des solutions.

BROUILLEUR GPS BLOQUANT UN AÉROPORT



2017

Transport

Nantes, France

Fiche 28



- **Impact**

Retards d'une heure et quart au décollage d'avions

- **Scénario d'incident**

Brouilleur GPS présent sur le parking de l'aéroport de Nantes perturbe les GPS des avions

- **Vulnérabilité**

Nature du système de communication GPS

BROUILLEUR GPS BLOQUANT UN AÉROPORT

Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Erreur

Complexité de l'attaque

Moyenne

Déroulement de l'attaque

- Un voyageur laisse son brouilleur GPS raccordé à l'allume-cigare de son véhicule stationné sur le parking de l'aéroport de Nantes.
- Le brouilleur bloque le GPS des avions de l'aéroport et empêche ainsi leur décollage.
- Les perturbations ont duré 1 h 15. Un camion-labo envoyé par l'agence nationale des fréquences, se trouvant à proximité de Nantes, a permis d'identifier le brouilleur.
- Le détenteur du brouilleur a été sanctionné par une amende de 2 000 € et a échappé à la prison car il s'agissait de sa première infraction de ce type.



Moyens mis en œuvre

- Brouilleur GPS

Enseignements à tirer, préconisations et contre-mesures

- Les systèmes GPS ne sont pas infallibles et sont vulnérables aux brouilleurs d'ondes. Il est important de **prendre en compte le brouillage des ondes radio** comme mécanisme de perturbation des opérations aéroportuaire. Ceci permettra d'identifier **les procédures de réaction en cas de compromission**.



- **Impact**

Certains bateaux ont reçu des informations erronées sur la position GPS pendant près d'un an

- **Scénario d'incident**

Outil pour leurrer les GPS

- **Vulnérabilité**

Nature des communications GPS

LEURRE DE GPS

Gravité de l'attaque

Faible

Motivation de l'attaquant

Stratégique inter-États

Complexité de l'attaque

Élevée



Déroulement de l'attaque

- Plusieurs bateaux au large du port de Shanghai recevaient des localisations GPS des autres navires incohérentes. Par exemple, certains navires étaient indiqués au large alors qu'ils étaient au port ou inversement.
- Les soupçons portent sur la présence d'un leurre GPS qui envoyait des informations erronées pour l'ensemble des bateaux sur le port.



Moyens mis en œuvre

- Leurre GPS



Enseignements à tirer, préconisations et contre-mesures

- **Les communications GPS ne sont pas authentifiées ni chiffrées.** Un leurre avec suffisamment de puissance peut surpasser les informations envoyées par les satellites. Le GPS du bateau prendra en compte uniquement le signal le plus proche.
- Étant donné l'étendue de la surface compromise (3 619 km²) et la durée des perturbations (un an), **les moyens mis en œuvre sont conséquents.**

BLOCAGE D'UN TÉLÉPHÉRIQUE PAR DES HACKERS

2018

Transport

Moscou, Russie

Fiche 30



- **Impact**

Évacuation des usagers et **mise à l'arrêt** du téléphérique pendant **2 jours**

- **Scénario d'incident**

Attaque ciblée de type **rançongiciel**

- **Vulnérabilité**

Intrusion dans le réseau et exploitation de vulnérabilités logicielles

BLOCAGE D'UN TÉLÉPHÉRIQUE PAR DES HACKERS

Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Financière

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- La société d'exploitation du Moscow Ropeway (MKD) aurait reçu une succession d'emails indiquant : « Des fichiers critiques hébergés sur le serveur central de la société ont été cryptés ». Une rançon en bitcoin était demandée, la somme réclamée augmentant avec le temps.
- La méthode de contamination initiale n'est pas connue ou communiquée.
- Un équipement similaire basé en Autriche a été découvert par des chercheurs comme étant directement visible depuis Internet.



Moyens mis en œuvre

- Rançongiciel



Enseignements à tirer, préconisations et contre-mesures

- Les attaques par ransomware sont de plus en plus communes. La sensibilisation des utilisateurs aux risques liés à la cybersécurité (méfiance dans les courriels, pièces jointes, liens à cliquer, etc.) est nécessaire afin de réduire la probabilité de ce type d'attaque, mais également d'en limiter l'impact (via la sensibilisation sur les indicateurs de compromission et les premières actions à réaliser en cas de compromission).
- Les mesures suivantes auraient permis de s'en prémunir :
 - **Sensibilisation** des utilisateurs sur les rançongiciels et les comportements à risque ;
 - **Cloisonnement** des réseaux industriels de tout autre réseau (IT ou Internet) ;
 - Application de manière régulière et systématique des **mise à jour de sécurité**.

DÉNI DE SERVICE SUR USINES AUTOMOBILES – ZOTOB

2005

Industrie

États-Unis d'Amérique

Fiche 31



- **Impact**

13 usines arrêtées pendant environ 1 heure,
50 000 travailleurs à l'arrêt (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

Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Attaque indifférenciée

Complexité de l'attaque

Faible



Déroulement de l'attaque

- Le ver **Zotob**, découvert en 2005, se diffuse sur Internet en exploitant des vulnérabilités présentes dans le protocole PnP (Plug and Play). 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



Enseignements à tirer, préconisations 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

2014

Industrie

Allemagne

Fiche 32



- **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

Gravité de l'attaque

Élevée

Motivation de l'attaquant

Financier ou Terroriste

Complexité de l'attaque

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 compromis 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
- Campagne ciblée d'emails infectés (*spear phishing*)



Enseignements à tirer, préconisations et contre-mesures

- La méthode d'attaque par *spear phishing* requiert des moyens importants et une bonne connaissance 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 **indépendants** du système de conduite.

PERTURBATION DU SYSTÈME DE PRODUCTION PAR VENGEANCE



2014

Industrie

Louisiane, USA

Fiche 33



- **Impact**

Ralentissement de la production et défaillance de certains systèmes (pertes chiffrées à 1,1 million de dollars)

- **Scénario d'incident**

Un administrateur SI licencié par son employeur de l'usine a utilisé de ses accès pour perturber le fonctionnement de la chaîne de production

- **Vulnérabilité**

Mauvaise gestion des contrôles d'accès

PERTURBATION DU SYSTÈME DE PRODUCTION PAR VENGEANCE



Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Vengeance

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Un administrateur SI d'une usine de fabrication de papier a été licencié le 14 février 2014.
- Quelques heures plus tard, l'usine a subi une attaque informatique perturbant les chaînes de production. L'attaque a continué pendant environ deux semaines.
- La police a perquisitionné la maison de l'ex-administrateur et a trouvé que son poste était connecté au réseau de l'usine et avait le contrôle des chaînes de production.
- L'ex-administrateur a plaidé coupable et a été condamné à une peine de 34 mois de prison.



Moyens mis en œuvre

- Accès administrateur non révoqué



Enseignements à tirer, préconisations et contre-mesures

- La gestion des accès des utilisateurs n'est pas uniquement de la responsabilité des services informatiques, mais de celle de plusieurs autres parties prenantes : ressources humaines et métiers. Sur le plan informatique, il est nécessaire de se préparer à la révocation des comptes. Cette préparation nécessite l'étude et la mise en place des comptes nominatifs (la révocation de comptes génériques a un impact plus important que celle d'un compte nominatif).
- Les mesures suivantes auraient permis d'éviter l'attaque :
 - **Révocation des comptes des personnels** n'intervenant plus sur le système industriel en lien avec les ressources humaines ;
 - Mise en place d'une authentification nominative pour les actions nécessitant un compte à haut privilège (l'accès à un compte générique nécessite une authentification nominative préalable) ;
 - Réalisation d'une **revue des droits d'accès** des prestataires aux systèmes ;
 - **Séparation des comptes à privilèges** de façon à les dissocier par rapport à leur besoin (par exemple la séparation des comptes d'administration, des comptes de maintenance).

TENTATIVE DE PERTURBATION DES INSTALLATIONS FRIGORIFIQUES

2019

Industrie

Montauban, France

Fiche 34



- **Impact**

Risque de perte de marchandises causée par la rupture de la chaîne du froid (le risque évalué à 500 000 euros)

- **Scénario d'incident**

Perturbation du fonctionnement des groupes frigorifiques par l'envoi de consignes malicieuses *via* des accès distants de maintenance

- **Vulnérabilité**

Défaut de contrôle d'accès logique, modifications en ligne des programmes d'automates, télémaintenance, absence de maîtrise des fournisseurs et prestataires

TENTATIVE DE PERTURBATION DES INSTALLATIONS FRIGORIFIQUES

Gravité de l'attaque
Faible

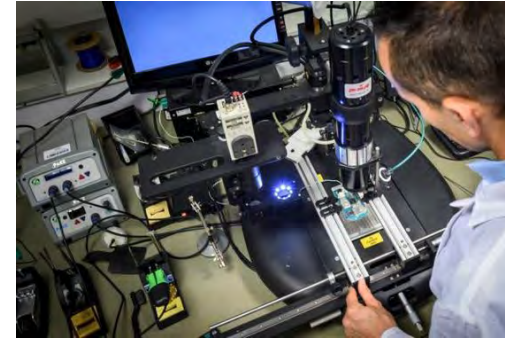
Motivation de l'attaquant
Vengeance

Complexité de l'attaque
Moyenne



Déroulement de l'attaque

- Une société industrielle a constaté que certains paramètres de ses équipements frigorifiques avaient été fortuitement modifiés, pouvant entraîner des dommages irréversibles sur les marchandises entreposées.
- Une première investigation interne a permis de démontrer l'implication d'une personne utilisant un compte de télémaintenance.
- Après avoir informé la société de télémaintenance des faits, cette dernière a informé la Gendarmerie nationale (N'Tech), qui, au cours de l'enquête, a retrouvé le terminal mobile personnel utilisé pour se connecter aux serveurs de l'entreprise visée.
- Il s'agirait d'un salarié éconduit de la société de maintenance informatique, qui aurait utilisé des comptes d'accès à distance à des fins malicieuses



Moyens mis en œuvre

- Un individu expérimenté ayant une connaissance des systèmes industriels ciblés



Enseignements à tirer, préconisations et contre-mesures

- Les accès à distance aux serveurs, s'ils sont parfois indispensables, augmentent fortement le risque d'attaque informatique. Ce risque est majoré si les comptes utilisés disposent de privilèges particuliers comme la modification de la configuration, la mise à jour logicielle...
- Les mesures suivantes permettent de protéger les installations :
 - **Révocation des comptes des personnels** n'intervenant plus sur le système industriel en lien avec les ressources humaines ;
 - Mise en place d'une authentification nominative pour les actions nécessitant un compte à haut privilège (l'accès à un compte générique nécessite une authentification nominative préalable) ;
 - Réalisation d'une **revue des droits d'accès** des prestataires aux systèmes ;
 - **Séparation des comptes à privilèges** de façon à les dissocier par rapport à leur besoin (par exemple la séparation des comptes d'administration, des comptes de maintenance).

DIVULGATION DE DOCUMENTS D'UNE CENTRALE NUCLÉAIRE

2014

Nucléaire

Corée du Sud

Fiche 35



- **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

Gravité de l'attaque

Faible

Motivation de l'attaquant

Politique/Financière

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Après une **campagne de spear phishing** (campagne de mails infectés) qui a touché **3 571 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 antinucléaire 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 ciblée d'emails infectés (*spear phishing*)
- Kimsuky est un logiciel malfaisant supposé utilisé par la Corée du Nord



Enseignements à tirer, préconisations 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 36



- **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



Gravité de l'attaque

Majeure

Motivation de l'attaquant

Stratégique inter-États

Complexité de l'attaque

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.



Enseignements à tirer, préconisations 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, etc.

INFECTION PAR VER DANS UNE CENTRALE NUCLÉAIRE – SLAMMER

2003

Nucléaire

Ohio, USA

Fiche 37



- **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

Gravité de l'attaque

Moyenne

Motivation de l'attaquant

Attaque indifférenciée

Complexité de l'attaque

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 qui le liait 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



Enseignements à tirer, préconisations 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 patches de sécurité**.

ARRÊT D'URGENCE D'UN RÉACTEUR NUCLÉAIRE

2008

Nucléaire

Hatch, Géorgie, USA

Fiche 38



- **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

Gravité

Moyenne

Motivation

Erreur

Complexité

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'information.**
- 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



Enseignements à tirer, préconisations 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.

DÉTOURNEMENT D'UN DRONE DE RECONNAISSANCE

2011

Défense

Iran

Fiche 39



- **Impact**

Récupération d'un drone « Sentinel » américain permettant le rétro-engineering et la 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

Élevée

Motivation de l'attaquant

Espionnage

Complexité de l'attaque

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

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



Enseignements à tirer, préconisations 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

2013

Distribution

États-Unis d'Amérique

Fiche 40



- **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



Gravité de l'attaque

Majeure

Motivation de l'attaquant

Financière

Complexité de l'attaque

Élevée



Déroulement de l'attaque

- Les pirates 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

- Campagne ciblée d'emails infectés (*spear phishing*)
- Utilisation du malware BlackPOS, de type RAM-scraping (trojan)



Enseignements à tirer, préconisations 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 réglementation (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 de 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).

ATTAQUE SUR UNE POMPE À INSULINE

2011

Santé

Monde

Fiche 41

Preuve de concept



- **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

Gravité de l'attaque

Faible

Motivation de l'attaquant

Sensibilisation

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Après l'analyse de la documentation constructrice (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 autres une application JAVA **non obfusquée** pour piloter 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'attaque : **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 »



Enseignements à tirer, préconisations 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 sûreté (safety)** comme dans les systèmes industriels classiques rendant une attaque potentiellement plus dangereuse.
- Les mesures suivantes permettent de sécuriser ce type 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.

RÉCOLTE D'INFORMATIONS SUR DES SYSTÈMES MÉDICAUX – ORANGEWORM

2018

Santé

Monde

Fiche 42



- **Impact**

Collecte d'informations sur les systèmes médicaux

- **Scénario d'incident**

Compromission de sociétés en lien avec le secteur de la santé, puis propagation du malware sur les systèmes de santé

- **Vulnérabilité**

Exploitation de systèmes obsolètes (Windows XP) et **absence de cloisonnement réseau**

RÉCOLTE D'INFORMATIONS SUR DES SYSTÈMES MÉDICAUX – ORANGEWORM

Gravité de l'attaque

Faible

Motivation de l'attaquant

Espionnage

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Un groupe d'acteurs malveillants nommé Orangeworm a lancé une attaque ciblant le secteur de la santé ainsi que les industries qui lui sont liées (Industrie manufacturière, logistique, agriculture, etc.).
- La groupe a utilisé un malware qui déployait une porte dérobée sur les machines infectées. Le malware a ainsi été retrouvé sur des équipements médicaux tels que des appareils de radiologie et des scanners.
- La porte dérobée permettait à l'attaquant de récolter des informations sur la machine et le réseau dans lequel elle se trouve afin de se propager.
- La propagation du malware n'était pas discrète : le malware exploitait des mécanismes connus, ciblait des systèmes obsolètes et cherchait à communiquer de façon continue avec les serveurs de contrôle et commande.



Moyens mis en œuvre

- Malware (Kwampirs)



Enseignements à tirer, préconisations et contre-mesures

- Les mesures suivantes auraient permis d'éviter l'attaque :
 - **Cloisonnement** du réseau afin de limiter la propagation de l'attaque ;
 - **Installation d'antivirus** sur les postes de pilotage des équipements ;
 - Mise en place de moyens techniques (par exemple, sondes) et organisationnels pour **détecter l'infection et réagir** ;
 - **Mise à jour dès que possible** des postes mobilisés pour l'utilisation de la machinerie médicale. Dès lors que la mise à jour n'est pas possible (absence de support, incompatibilité, etc.), il est important de mettre en place des mesures de durcissement et de défense périmétrique.

PRISE DE CONTRÔLE DES SIRÈNES D'URGENCE

2017

Sûreté

Dallas, Texas, USA

Fiche 43



- **Impact**

Saturation des dispositifs d'urgence (4 400 appels), panique citoyenne, volume sonore très important, pendant 1 h 30

- **Scénario d'incident**

Prise de contrôle du système de gestion des sirènes d'urgence

- **Vulnérabilité**

Manque de protection des équipements de communication, et de leur protocole

PRISE DE CONTRÔLE DES SIRÈNES D'URGENCE

Gravité de l'attaque

Élevée

Motivation de l'attaquant

Par challenge

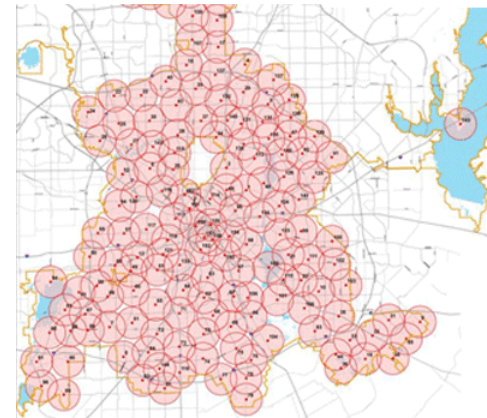
Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Dans la nuit du 7 au 8 avril 2017, entre 23 h 40 et 1 h 20, l'ensemble des 156 sirènes d'urgence de Dallas sonnent l'alerte. Ces sirènes sont habituellement utilisées pour prévenir de dangers météo (ex. : tornades).
- La municipalité a d'abord cru à un dysfonctionnement, mais il s'agissait bien d'un piratage par un hacker encore inconnu à ce jour.
- Le système de contrôle des sirènes fonctionne par l'activation de commandes envoyées par simple signal radio (DTMF/AFSK — bande 700 MHz). Le hacker aurait eu accès aux documentations du système d'alerte et aurait ainsi envoyé la commande d'activation, ou aurait rejoué le signal utilisé lors des tests d'alarme mensuels.
- Les alarmes ont cessé de retentir lorsque le système complet a été arrêté.



Implantation des 156 sirènes de Dallas



Moyens mis en œuvre

- Système d'émission radio
- Écoute et reproduction du code de déclenchement des signaux d'alarme



Enseignements à tirer, préconisations et contre-mesures

- Le système d'alerte d'urgence de la ville de Dallas était obsolète : l'équipement, mis en service plus d'une dizaine d'années auparavant, n'avait pas été évalué face au risque cyber.
- De plus, le protocole utilisé par le système n'était pas sécurisé : le rejeu du signal d'alerte aurait permis d'activer les sirènes.
- Les mesures suivantes auraient permis de s'en prémunir :
 - **Chiffrement des communications ;**
 - **Gestion de l'obsolescence.**
- Note : Deux ans après cet incident, les systèmes d'alerte de tornade de deux villes du comté de Dallas ont subi une attaque identique. Afin d'arrêter les 30 sirènes enclenchées durant la nuit, les systèmes ont été désactivés. Cette désactivation a été faite la veille d'importants orages et risques de tornades sur la région.

BLOCAGE DU SYSTÈME DE CONTRÔLE D'ACCÈS AUX CHAMBRES

2017

GTB

Autriche

Fiche 44

Source d'informations limitée



- **Impact**

Atteinte à l'image de marque de cet hôtel de luxe.

La direction de l'hôtel a accepté de payer plusieurs rançons allant jusqu'à des valeurs de deux bitcoins (environ 1 600 € à l'époque)

- **Scénario d'incident**

Les ordinateurs gérant la programmation des cartes d'accès aux chambres d'un hôtel ont été touchés par un rançongiciel

- **Vulnérabilité**

Manque de sensibilisation des utilisateurs

BLOCAGE DU SYSTÈME DE CONTRÔLE D'ACCÈS AUX CHAMBRES

Gravité de l'attaque

Faible

Motivation de l'attaquant

Financière

Complexité de l'attaque

Moyenne



Déroulement de l'attaque

- Plusieurs vagues d'attaque par rançongiciel ont eu lieu entre les mois de décembre 2016 et de janvier 2017 (quatre vagues officiellement annoncées).
- Le 22 janvier 2017, l'attaque a bloqué les ordinateurs gérant les réservations, la facturation des clients ainsi que la création des cartes d'accès aux chambres.
- À chaque demande de rançon, le directeur général de l'hôtel a dû payer une rançon de deux bitcoins (environ 1 600 € à l'époque).
- Personne n'a été enfermé dans sa chambre.



Moyens mis en œuvre

- Campagne ciblée d'emails infectés (*spear phishing*) utilisant un acteur connu et considéré fiable (Telekom Austria)
- Malware à utilisation large spectre
- Social engineering



Enseignements à tirer, préconisations et contre-mesures

- Le paiement d'une rançon n'est pas une garantie pour récupérer les fichiers compromis ni arrêter d'être victime d'une attaque.
- Les utilisateurs doivent être sensibilisés au risque que représente le *spear phishing* (campagne de mails infectés).
- L'utilisation d'une sous-traitance spécialisée pour effectuer le maintien en condition de sécurité doit être envisagée si les ressources internes ne sont pas présentes.
- Les mesures suivantes auraient permis de s'en prémunir :
 - Blocage des macros Office et sensibilisation des employés à la sécurité ;
 - Cloisonnement plus important des réseaux ;
 - **Mise en place d'un mécanisme de liste blanche** au niveau des applications utilisables par les stations et serveurs (voire la mise en place d'un mécanisme de durcissement des postes) ;
 - Stockage de sauvegardes des systèmes sur des dispositifs non connectés aux réseaux.



PRÉSENTATION DU CLUSIF

PRÉSENTATION DU CLUSIF

Le Clusif est l'association de référence de la **sécurité du numérique** en France à travers ses **conférences** thématiques et les **publications** de ses groupes de travail.

Il réunit en parfaite équité au sein de deux collèges, offreurs et utilisateurs, tous les secteurs d'activité autour de la **cybersécurité** et de la confiance numérique.

Le Clusif, c'est aussi :

- © Le *Panorama de la cybercriminalité* – **#Panocrim**
- © L'étude *Menaces informatiques et pratiques de sécurité en France* – **#MIPS**
- © L'exercice de cybercrise ÉCRANS

Le réseau du Clusif réunit les **Clusir**, associations partenaires qui relaient les actions du Clusif dans les régions et à l'international

Plus d'infos sur clusif.fr



CRÉDIT PHOTO

CRÉDIT PHOTO

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

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

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

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

<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

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

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

https://commons.wikimedia.org/wiki/File%3ACANDU_at_Qinshan.jpg

Atomic Energy of Canada Limited [Attribution], via Wikimedia Commons

[https://commons.wikimedia.org/wiki/File%3AWolsong_\(04790183\).jpg](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

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

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

<http://www.water-technology.net/projects/delta-mendota-canal-california-aqueduct-intertie/delta-mendota-canal-california-aqueduct-intertie1.html>

Anthony DUNN

<http://www.adunnphotography.com/media/55fc9b6b-d79d-40c7-883d-cbe6857ebbb-tehama-colusa-canal-1>

[https://commons.wikimedia.org/wiki/File%3ATarget_West_Reynolds_Road_Lexington%2C_KY_3_\(9_568_771_360\).jpg](https://commons.wikimedia.org/wiki/File%3ATarget_West_Reynolds_Road_Lexington%2C_KY_3_(9_568_771_360).jpg)

By Mike Kalasnik from Fort Mill, USA [CC BY-SA 2.0 (<http://creativecommons.org/licenses/by-sa/2.0/>)], via Wikimedia Commons

<https://blog.kissmetrics.com/gamification-for-better-results/>

<https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

<https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

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

[https://commons.wikimedia.org/wiki/File%3ADavis-Besse_Nuclear_Power_Station_cooling_tower_\(4183\).jpg](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

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

<http://www.eham.net/classifieds/detail/335053>

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

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

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

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

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

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

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

https://commons.wikimedia.org/wiki/File%3ARQ-170_Wiki_contributor_3Dartist.png

© TruthDowser/Wikimedia Commons, در ویکی‌انبار

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

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

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

<http://toastytech.com/guis/win98.html>

CRÉDIT PHOTO

[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+\(Titel\)](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))

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

<http://www.alalam.ir/news/1648514>

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

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

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

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

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

<http://kitprofs.com/services/water/>

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

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

<http://coursierstrategie.com/4899-russie-construction-des-reacteurs-nucleaires-en-iran.html>

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

<http://flaticon.com>

<https://www.symantec.com/blogs/threat-intelligence/wannacry-rancongiciel-attack>

<https://www.bbc.com/news/health-39899646>

<https://www.wired.co.uk/article/austria-hotel-rancongiciel-true-doors-lock-hackers>

<https://www.forbes.com/sites/leemathews/2017/01/30/hackers-lock-down-hotel-rooms-in-a-new-twist-on-ransom-attacks/#5adacd204664>

<https://www.newsbtc.com/2017/01/30/romantik-seehotel-jaegerwirt-bitcoin-ransom>

<https://www.blackhat.com/docs/us-17/wednesday/us-17-Lee-Industroyer-Crashoverride-Zero-Things-Cool-About-A-Threat-Group-Targeting-The-Power-Grid.pdf>

https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

https://cdn.pixabay.com/photo/2016/08/04/10/13/resin-1568726_960_720.jpg

<https://pixabay.com/fr/photos/t%C3%A9l%C3%A9ph%C3%A9riques-ascenseur-de-ciel-1246615/>

<https://www.cybersecurity-review.com/cyber-and-the-healthcare-industry/>

https://fr.m.wikipedia.org/wiki/Fichier:IRM_3T_clinique_NeuroSpin.jpg

<https://www.wired.com/story/wind-turbine-hack/>

<https://www.marketscreener.com/A-P-M-LLER-M-RSK-1412885/news/A-P-M-ller-M-rsk-Maersk-shares-plummet-on-bleak-outlook-as-trade-war-looms-28042693/>

<https://www.philly.com/philly/business/merck-is-the-target-of-a-massive-hack-20170627.html>

<https://www.silicon.fr/saint-gobain-notpetya-250-manque-a-gagner-181637.html>

<https://www.independent.co.uk/life-style/gadgets-and-tech/news/petya-cyber-attack-affected-companies-hack-wpp-rosneft-mondelez-deutsche-post-security-problems-a7811056.html>

<https://www.sott.net/article/354866-Petya-ransomware-attack-spreads-globally-targets-include-Merck-in-US>

https://media.wired.com/photos/59266054cfe0d93c4742ffd0/master/w_582,c_limit/Tornado-SirenTA_GettyImages-555017489.jpg

https://1.bp.blogspot.com/-G1-6BQSojWc/WO9fAl3V3pl/AAAAAAAAAMl/hFih381Fc90oOkwj02rtY7yY1aa_HRvQgCLcB/s728-e100/emergency-tornado-siren-hack.png

<https://pxhere.com/fr/photo/994596>

https://www.flickr.com/photos/lauri_/8269372762/

<https://france3-regions.francetvinfo.fr/centre-val-de-loire/indre/carburants-indre-situation-nouveau-normale-1334955.html>

https://motherboard.vice.com/en_us/article/43qkgb/flaws-in-gas-station-software-let-hackers-change-prices-steal-fuel-erase-evidence

https://archerint.com/computer-guy-sabotaged-factory-heads-prison/?utm_content=buffer620a3&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

https://archerint.com/computer-guy-sabotaged-factory-heads-prison/?utm_content=buffer620a3&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

https://www.theregister.com/2017/07/27/killer_car_wash/

<https://www.securityweek.com/tesla-model-x-hacked-chinese-experts>

CRÉDIT PHOTO

<https://zdnet2.cbsistatic.com/hub/i/2019/10/31/8712b91c-2d7c-43e3-85bc-db551effb317/wind-solar-energy.jpg>

https://www.eenews.net/image_assets/2019/10/image_asset_65935.jpg

<https://www.ladepeche.fr/2020/08/26/lex-salarie-avait-pirate-le-systeme-informatique-9034689.php>

<https://www.gendinfo.fr/dossiers/la-menace-cyber/Des-technicites-alliees-a-l-investigation>

<https://www.databreachtoday.com/exclusive-vulnerabilities-could-unlock-brand-new-subarus-a-9970>

<https://www.databreachtoday.com/exclusive-vulnerabilities-could-unlock-brand-new-subarus-a-9970>

<https://www.moneyvox.fr/actu/76621/avion-les-collisions-au-sol-ou-avec-des-oiseaux-content-tres-cher-aux-assurances>

<https://www.ouest-france.fr/pays-de-la-loire/nantes-44000/son-bouilleur-de-gps-avait-bloque-l-aeroport-de-nantes-5179999>

<https://www.france24.com/fr/20191118-gps-leurrage-shanghai-mit-chine-mystere-port-bateau>

<https://www.ouest-france.fr/pays-de-la-loire/nantes-44000/son-bouilleur-de-gps-avait-bloque-l-aeroport-de-nantes-5179999>

<https://pylos.co/2021/02/09/water-water-everywhere-but-nary-a-hacker-to-blame/>

<https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-olds-mars-water-supply-during-hack-sheriff-says/>

<https://france3-regions.francetvinfo.fr/centre-val-de-loire/indre/carburants-indre-situation-nouveau-normale-1334955.html>

https://motherboard.vice.com/en_us/article/43qkqb/flaws-in-gas-station-software-let-hackers-change-prices-steal-fuel-erase-evidence

https://archerint.com/computer-guy-sabotaged-factory-heads-prison/?utm_content=buffer620a3&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

https://archerint.com/computer-guy-sabotaged-factory-heads-prison/?utm_content=buffer620a3&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

https://www.theregister.com/2017/07/27/killer_car_wash/

<https://www.securityweek.com/tesla-model-x-hacked-chinese-experts>

<https://zdnet2.cbsistatic.com/hub/i/2019/10/31/8712b91c-2d7c-43e3-85bc-db551effb317/wind-solar-energy.jpg>

https://www.eenews.net/image_assets/2019/10/image_asset_65935.jpg

<https://www.ladepeche.fr/2020/08/26/lex-salarie-avait-pirate-le-systeme-informatique-9034689.php>

<https://www.gendinfo.fr/dossiers/la-menace-cyber/Des-technicites-alliees-a-l-investigation>

<https://www.databreachtoday.com/exclusive-vulnerabilities-could-unlock-brand-new-subarus-a-9970>

<https://www.databreachtoday.com/exclusive-vulnerabilities-could-unlock-brand-new-subarus-a-9970>

<https://www.moneyvox.fr/actu/76621/avion-les-collisions-au-sol-ou-avec-des-oiseaux-content-tres-cher-aux-assurances>

<https://www.ouest-france.fr/pays-de-la-loire/nantes-44000/son-bouilleur-de-gps-avait-bloque-l-aeroport-de-nantes-5179999>

<https://www.france24.com/fr/20191118-gps-leurrage-shanghai-mit-chine-mystere-port-bateau>

<https://www.ouest-france.fr/pays-de-la-loire/nantes-44000/son-bouilleur-de-gps-avait-bloque-l-aeroport-de-nantes-5179999>

<https://pylos.co/2021/02/09/water-water-everywhere-but-nary-a-hacker-to-blame/>

<https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-olds-mars-water-supply-during-hack-sheriff-says/>

<https://www.se.com>