

The image features the IBM logo, which consists of the letters 'IBM' in a bold, sans-serif font. Each letter is composed of eight horizontal white stripes of equal thickness, set against a dark blue background that has a subtle gradient from top to bottom. The logo is centered horizontally and vertically within the frame.

La sécurité des objets connectés (IoT & OT)

Croissance des attaques, criticité de l'adhésion ComEx, mise en place chez IBM



Sébastien Jardin

Directeur du Business Development

IBM Security France

Membre du CLUSIF

<https://www.ibm.com/security>

Qui est IBM Security

- Fournisseur mondial de cybersécurité d'entreprise
- 14 segments couverts en cybersécurité
- Chiffre d'affaires 2018 de \$2Mds et en croissance
- 8 000+ employés en sécurité
- 10k+ brevets de sécurité

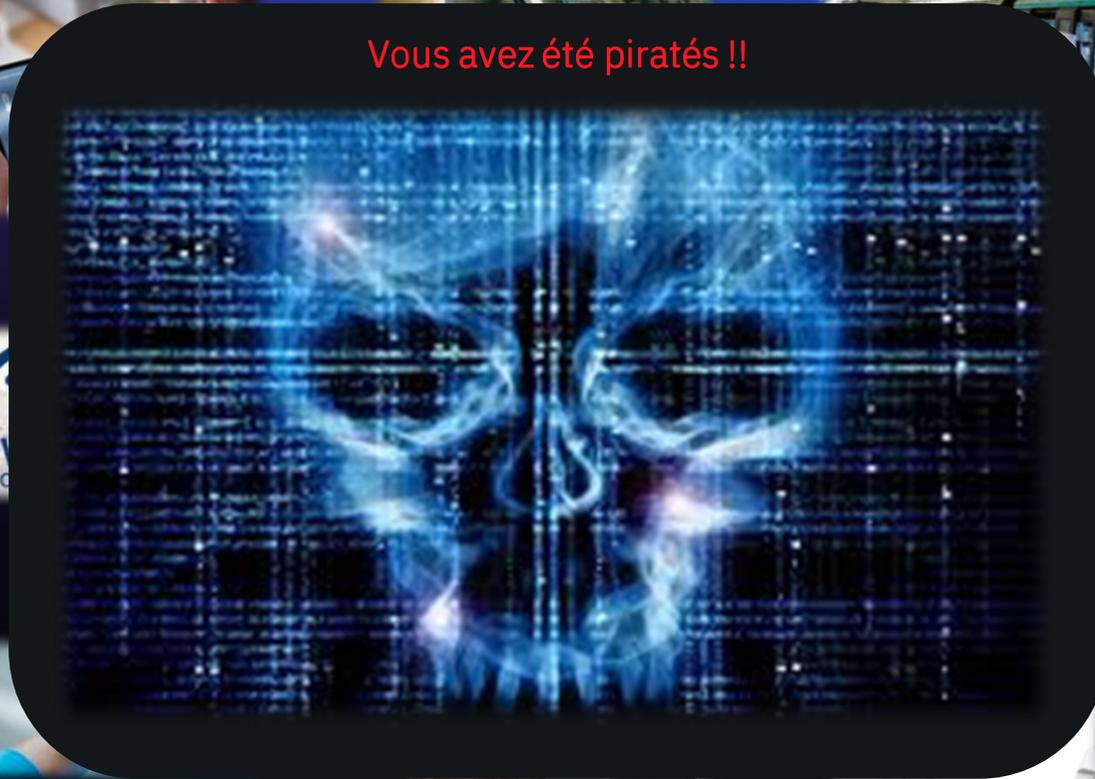


La digitalisation est une vague déferlante très utile...



... mais qui peut se retourner rapidement contre ses créateurs

Vous avez été piratés !!



Les attaques ont majoritairement une motivation financière

X-Force Threat Intelligence Index²⁰²⁰

Top 10 industries targeted

Top 10 targeted industries ranked by attack volume, 2019 vs. 2018 (Source: IBM X-Force)

Sector	2019 rank	2018 rank	Change
Financial Services	1	1	-
Retail	2	4	2
Transportation	3	2	-1
Media	4	6	2
Professional services	5	3	-2
Government	6	7	1
Education	7	9	2
Manufacturing	8	5	-3
Energy	9	10	1
Healthcare	10	8	-2

Données monétisables

Services Financiers, Commerce de Détail, Transports,
Médias, Services Professionnels, Gouvernement, Education,
Fabrication, Energie, Santé

Actions monétisables

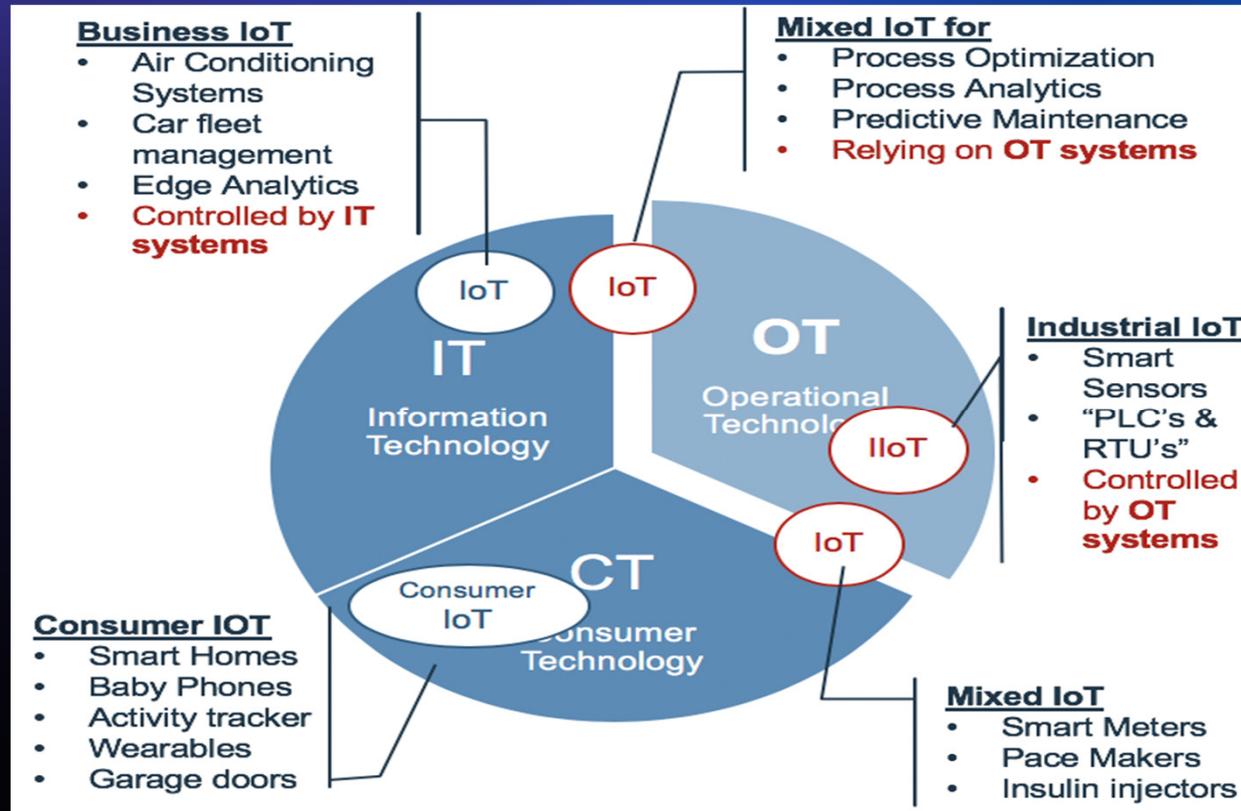
Services Financiers, Commerce de Détail, Transports,
Médias, Services Professionnels, Gouvernement, Education,
Fabrication, Energie, Santé

Influence & Déstabilisation

Médias, Gouvernement



IoT & OT... de quoi parle-t-on ?





Dans toutes les entreprises

Source :  ARMIS



SYRINGE PUMP

ULTRASOUND

PATIENT MONITOR

COMPROMISED DEVICE

⚠ Device behavior shows signs of compromise. Recommend quarantine and shut off the device. Then review for security.

TABLET

PATIENT MONITOR

INFUSION PUMP

COMPROMISED DEVICE

⚠ Device behavior shows signs of compromise. Recommend quarantine and shut off the device. Then review for security.

MEDICAL LAPTOP

Dans le monde médical

Source : 



ROBOTIC ARM 1

SECURITY CAM

SECURITY CAM

HVAC SENSOR

ACCESS POINT

TABLET

TABLET

HMI

ROBOTIC ARM 2

ROBOTIC ARM 3

COMPROMISED DEVICE

Device behavior shows signs of compromise. Botnet or Ransomware activity. Recommend quarantine and shut off the device. Then review for security.

SENSOR

TABLET

TABLET

RFID SCANNER

Dans le monde industriel

Source : 

IoT & OT – Une nouvelle cible plébiscitée par les pirates



2000%

Hausse du nombre d'attaques entre 2018 et 2019 visant l'OT et l'IoT.

Hardware & Mots de passe

La plupart des attaques observées étaient centrées des vulnérabilités connues dans les matériels en place et utilisaient la technique de « brute force ».

Convergence IT/OT

Les pirates continuent de se tourner vers différents vecteurs d'attaque, avec un ciblage accru des appareils IoT, de la technologie opérationnelle (OT) et des systèmes industriels ou médicaux connectés.

IoT & OT – Les entreprises attaquées via les consommateurs

Figure 2:

Consumer vs. enterprise IoT attacks

Monthly volume of consumer vs. enterprise IoT attacks in 2019 (Source: IBM X-Force)



38 milliards

d'objets connectés en 2020, ce qui explique l'intérêt des pirates pour ce vecteur avec des rebonds de type malwares ou des scripts automatisés.

Point de bascule

2019 a connu une forte accélération des attaques sur les composants électroniques grand public vers les systèmes de l'entreprise (cf. accès réseau, BYOD...).

Identité & Accès

Les IoT & OT ont une activité souvent automatisée et opèrent en « machine to machine » ce qui rend crucial leur incorporation à l'infrastructure IAM de l'entreprise.

La sécurité de l'IoT et de l'OT est un domaine encore jeune



Sécurité IT	Sujet	Sécurité OT / IoT
Conformité Financier	Risques enjeux	Sûreté / Ecologie Vies humaines Conformité
3 à 5 ans	Cycle de vie	5 à 20 ans
Fréquents	Changements	Rares
Accepté	Interruption pour mesure de sécurité	Interdite
Fréquent	Patching	Rare et complexe (accord + tests)
IP / Zoning	Réseau	Début d'IP Spécif / analogiques
Moyennes à fortes. Maturité.	Compétences spécifiques en sécurité IT.	Pas ou peu. Sujet naissant.
Génériques et partageables.	Cas d'usage (attaques...)	Très liés aux métiers.



L'impact sur les entreprises et les humains peut être colossal...

Hackers 'hit' US water treatment systems

21 November 2011 | Technology

Hackers are alleged to have destroyed a pump used to pipe water to thousands of homes in a US city in Illinois.

Hackers with access to the utility's network are thought to have broken the pump by turning it on and off quickly.

The FBI and Department for Homeland Security (DHS) are investigating the incident as details emerge of what could be a separate second attack.



The alleged attack was made on a system that piped clean water to homes in Illinois.

Hackers Attack Safety System, Shut Down Plant

Dec 15, 2017



By Editors of Power Engineering

Makers of industrial software confirmed the operations of a plant was halted by a **cyberattack** by hackers likely working for a national government.

Reuters reported the attack targeted Triconex industrial safety technology from Schneider Electric SE.

Schneider, as well as cybersecurity company FireEye, confirmed the attack but did not identify the victim, industry or location of the attack. Security company Dragos said the target was somewhere in the Middle East, while CyberX said the victim was in Saudi Arabia.

The UK's power grid and water supply may have been hit by hackers

Security

An advisory warning suggests "state-sponsored hostile threat actors" have been targeting infrastructure IT systems

Adam Shepherd
18 Jul 2017



Facebook, Twitter, Google+, LinkedIn, Email, Print icons.

Proof-of-concept ransomware to poison the water supply

BY GRAHAM CLULLEY POSTED 15 FEB 2017 - 02:23PM

CyberSecurity



L'USINE DIGITALE

[FIC 2017] Le patron de l'ANSSI craint des morts à cause des objets connectés (Janvier 2017)



Victime d'une cyberattaque d'ampleur mondiale, le groupe Renault a décidé de mettre plusieurs de ses sites à l'arrêt. (Mai 2017)

LE FIGARO tech JDN

Un virus informatique paralyse un hôtel de luxe en Autriche (Janvier 2017)



Triton: ce malware a visé un système de contrôle industriel de Schneider Electric (Janvier 2018)

... et parfois vous participerez à une attaque sans le savoir

LE MAGAZINE DES OBJETS CONNECTÉS ET INNOVANTS
OBJETCONNECTE.NET

Un hacker pirate un casino via le thermomètre connecté d'un aquarium (Avril 2018)

Oct 2016 : DDoS on Dyn impacts Twitter, Spotify and others

'Smart home devices used as weapons in website attack'



BBC

NEWS

Siecle Digital

Une fois piratée, une montre connectée pour seniors pouvait mener à la surdose médicamenteuse (Juillet 2020)

Commencez par les sujets non négociables et leurs risques

Humains

- Erreur humaine
- Inconscience
- Malice
- Ingénierie sociale
- Espionnage
- Détournement de mot de passe
- Sabotage
- Écoute
- Fraude physique
- Interception
- Vol physique
- Faible recyclage
- Chantage

Légaux

- RGPD
- Signature électronique
- Gestion des archives
- Bâle III
- ...

Techniques

- Matériel
- Logiciel
- Environnement

- Virus
- Vers
- Cheval de Troie
- Porte dérobée
- Spyware
- Enregistreur de frappe
- Exploit
- Rootkit
- Faux logiciel
- Bombe logique
- Spam
- Hameçonnage
- Canular
- ...

Chez IBM, la sécurité IoT & OT est suivie au niveau ComEx



Pentesters IBM

« Cassez tout ce que vous pouvez, volez tout ce que vous pouvez. Il vaut mieux identifier les failles en amont que les découvrir suite à une attaque.

Cette façon de faire est discutée et approuvée par le top management. »

Former IBM Global CISO

Faire de la sécurité un réflexe métier est un travail quotidien



Parler le langage du ComEx

La mission du RSSI est de protéger l'entreprise et ses clients des menaces digitales. Parler le langage des métiers permet de se positionner en partenaire facilitateur et pas en contrainte.

1



Avoir une approche holistique du risque

Votre temps, équipe et budget ne seront jamais suffisants pour adresser tous les sujets, et éviter de créer des silos métiers vous permettra d'optimiser l'usage de vos ressources au global.

2



Répandre la culture sécurité

Vous ne pourrez jamais réaliser la protection digital seuls, vous avez besoin d'être expert en technologies mais aussi capable de faire des métiers la première ligne de cyberdéfense.

3

IBM France, Telecom Valley et Security by Design

- ❑ La R&D d'IBM pense & développe en mode « Security by Design », **IBM France Lab implanté depuis des années à Sophia-Antipolis**
- ❑ Participation de **Patrick Merlin** au 3^e Sophia Security Camp « *Mise en place du Process SPbD dans les différentes équipes de développement au Lab R&D d'IBM (Paris , Sophia ...) SPbD -Threat Model -Code Scan (SAST, DAST, IAST, Other) -Security Tests -Pen Test (internal vs external) -Vulnerability management SPbY on legacy code VS new software* » (8 Octobre 2019)
- ❑ Participation active des collaborateurs IBM dans les **communautés de Telecom Valley**

IBM Security

Merci



FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  ibm.com/security/community
-  www.securitylearningacademy.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

