

# Ransomwares, attaques ciblées & data breach : Comment protéger votre activité

Présenté par Adrien Ottavino

# AXES DE DISCUSSION

---

- Les différents cas d'attaques : Industroyer, British Airways, Lojax, Asco, Agent Smith, Marriott, Capital One
- Quid des vulnérabilités ?
- Les moyens de se protéger
- Conclusion



# 1. ÉTAT DES LIEUX D'UNE SITUATION PRÉOCCUPANTE

LES DIFFÉRENTS CAS D'ATTAQUES

# 1h

C'est le temps passé, pour des milliers de personnes, sans électricité en Ukraine après l'attaque **Industroyer**.



Décembre 2016 : La plus grosse cyberattaque industrielle, 250 000 foyers impactés.

# 380 000

C'est le nombre de personnes touchées suite à l'attaque menée par le groupe **Magecart** ciblant British Airways.



Juillet 2018 : Un script récupérait les données utilisateurs provenant d'achats en ligne.

# 110 millions

C'est le montant (en €) de la sanction que veut infliger l'Information Commissioner's Office au groupe hôtelier Marriott suite à une fuite de données.



Septembre 2018 : Le manquement à la protection des données privées implique une lourde sanction

# LOJAX

C'est le premier Rootkit UEFI  
découvert dans la nature par ESET.



Septembre 2018 : Une attaque perpétrée par Sednit, Lojax a été déployé à distance.

# 3 semaines

C'est la durée pendant laquelle 1000 personnes étaient au chômage technique suite à l'arrêt de la production du sous-traitant Asco.



Juin 2019 : Un ransomware infecte les systèmes IT puis les systèmes de production, stoppant l'activité.



# 25 millions

C'est le nombre d'utilisateurs Android infectés par **Agent Smith** un malware diffusé via des publicités malveillantes.



Juillet 2019 : Un malware imite "Whatsapp" sur 9apps.com et récupère les données privées des utilisateurs.

# 106 millions

C'est le nombre de victime de la fuite de données subie par Capital One aux USA et au Canada.



Juillet 2019 : Un hacker pirate les systèmes de Capital One en mars ; le groupe le découvre en juillet.


# COMBIEN D'INCIDENTS SUPPLÉMENTAIRES POUR QUE LES ENTREPRISES RÉAGISSENT ?



# 2. QUID DES FAILLES ?

LES TYPES DE VULNÉRABILITÉS

# LES FAIBLESSES MAJEURES



## VULNÉRABILITÉS DES SYSTÈMES

- Mises à jour système
- Solutions défectueuses ou inadaptées



## SÉCURITÉ DES ACCÈS

- Mots de passe faibles
- Sessions à distances non protégées et ouvertes



## L'UTILISATEUR

Le maillon faible de la sécurité, trop peu éduqué il présente un vrai risque pour l'activité

# 3. LES MOYENS DE SE PROTÉGER

SOLUTIONS & BONNES PRATIQUES

## **ANTIMALWARE**

Protection multi-couche

## **BACKUP**

En externe et en interne

## **FIREWALL**

Hardware et Software

## **THREAT INTELLIGENCE**

Prévoir et anticiper les menaces

## **SANDBOXING**

Répliquer l'environnement  
réseau

## **ENCRYPTION**

Protéger les données et les  
rendre inaccessibles

## **EDR**

Surveiller et analyser  
l'ensemble des activités

## **MFA**

Sécurité des accès, isoler le  
facteur risque

# LES 3 PILLIERS DE LA SÉCURITÉ



## SÉCURITÉ RÉSEAU/PÉRIPHÉRIQUE

Mettre en place un système de protection multicouche visant à sécuriser au mieux les machines du réseau contre les attaques.



## SÉCURITÉ DES DONNÉES

Rendre les données inaccessibles pour garantir leur intégrité même en cas de fuite.



## SÉCURITÉ DES ACCÈS

Sécuriser l'accès pour les machines et utilisateurs.





# CONCLUSION

SÉCURISER, ORGANISER, ÉDUQUER

**“ Montrez aux gens les problèmes, puis montrez-leur les solutions : ils seront incités à agir. ”**

- BILL GATES

MERCI  
POUR  
VOTRE  
ATTENTION

