# Quand le PC du RSSI disparaît…

Nicolas GENET (ARIADNEXT)

# Introduction

## Présentation de l'intervenant

- Nicolas GENET,  RSSI de la société ARIADNEXT
- ARIADNEXT est spécialisé dans la vérification d'identité à distance, prestataire de services de confiance (qualifié RGS* et certifié eIDAS) et fournisseur d'identité pour France Connect

## Pourquoi cette intervention ?

- Retour d'expérience **rentrant** pleinement dans le thème d'aujourd'hui…
- …tout en **sortant** de l'ordinaire : un scénario digne d'un roman !
- Un RETEX à la croisée des mondes de **l'humain**, du **juridique** et de la **technique**
- Des enseignements riches et nombreux, à partager avec l'auditoire

# Avant de continuer

Cette restitution a été préalablement approuvée par la Direction de la société 😉

# Les faits

## Contexte

- Période d'essai sur un poste à responsabilité
- Événements personnels périphériques
- Prix du PC élevé

## Chronologie

- 29/03/2018 → Vol du PC au domicile
- 31/03/2018 → Clôture de l'incident de sécurité
- 18/04/2019 → Retour d'expérience public

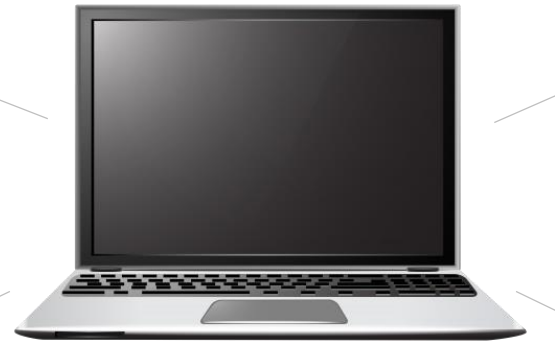
## Certitudes

- Impact sur la crédibilité du RSSI
- Source de risque (au sens de la méthode EBIOS RM)

# Anatomie de l'objet volé

**Chiffrement matériel OFF**

**Prix élevé**
(env. 2000 €)



**Chiffrement à la donnée ON**

- Données client AVV
- Données internes sensibles
- Autres données ⚠

**Contenu dans une sacoche**

- Documents papier
- Pas d'élément d'authentification matériel (ex: clé RSA SecurID)

**Dispositif anti-vol OFF**
(disponible sur certains modèles seulement)

# Actions immédiates

## Révocation des accès

- Accès liés à l'entreprise (services accessibles à partir du compte LDAP)
- Accès personnels (LinkedIn, mail perso)

## Notification hiérarchie

- Pas une partie de plaisir !

## Dépôt de plainte

- Fait marquant : le mari de l'Officier de Police est... RSSI
- N'a pas abouti

## Inventaire des actifs

- Besoin en confidentialité
- Besoin en disponibilité
- Y compris le contenu de la sacoche

## Achat PC

- Commande d'un PC de même modèle

# Actions à froid

## Enquête de voisinage

- Interviews avec les voisins de l'étage
- Affichage d'un mot personnalisé dans le hall d'entrée

## Migration des données

- Restauration d'une partie des données sauvegardées
- Poste de travail temporaire

## Saisie fiche incident

- Incident sans impact sur les clients → Fiche interne

## Tentative de localisation

- Fonctionnalité « anti-theft »
- Connexions à la Box Internet du domicile

## Parcours sites de revente

- Sites bien connus
- Facteur défavorable : conditions de rachat des objets de valeur

# Avant de continuer

**PC retrouvé !**

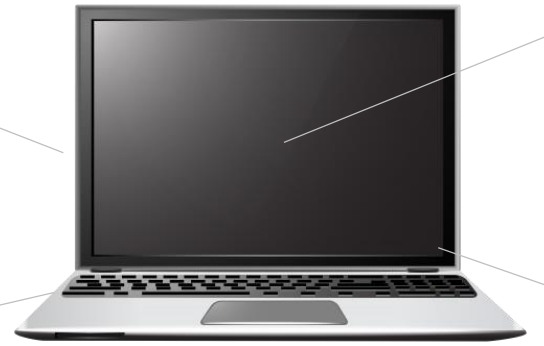
Jeudi 29 mars 08h05 → Samedi 31 mars 21h50

Clôture de l'incident au bout de **62 heures**

# Un peu de forensics

Profil de l'attaquant :

**Malveillant pathologique** (postulat)



1 **Examination visuelle**
(état, traces de doigt, sacoche)

2 **Désactivation Wi-Fi**
(machine + Box)

4 **Analyse des journaux d'événements Windows**
Pas de boot du PC

3 **Observation voyant de charge**
Indicateur pertinent

# Capitalisation

## Mesures organisationnelles

- Insistance sur le risque de vol/perte pendant les sensibilisations
- Warning événements externes (ex : événements communautaires)
- Sacoche plus loin de la porte

## Mesures techniques

- Chiffrement matériel de tous les postes de travail ARIADNEXT depuis
- Sauvegardes plus régulières
- Verrou de la porte d'entrée même si chez soi pour 5 minutes !

# Enseignements

**Un exemple qui illustre parfaitement ce que nous dit la théorie sur les incidents de sécurité…**

- **On ne sait jamais tout** sur un incident de sécurité (mode opératoire, source de menace, etc.)… même un an après un incident de sécurité
- La **menace interne** ne doit jamais être écartée : le danger est parfois très proche…
- La **sécurité physique** ne doit jamais être sous-dimensionnée (rappel : il s'agit de la 1ère couche du modèle de défense en profondeur appliqué aux SI)
- Analogie possible entre les accidents aériens et les incidents de sécurité du SI
- Nous ne sommes **jamais trop préparés à un incident de sécurité**. Même si les procédures sont formalisées et les typologies identifiées, chaque incident est différent.
- On peut (doit !) ressortir **plus fort** d'un incident de sécurité.