VICTIME D'UN RANSOMWARE ?

RÉCUPÉREZ VOS DONNÉES AVEC

DATABACK

Samuel Durand
Directeur technique
DataBack

DATABACK
RÉCUPÉRATION DE DONNÉES

QUELLES OPTIONS POUR RESTAURER MES DONNÉES ?

SI VOS SAUVEGARDES SONT IMPACTÉES

01

DATABACK, LABORATOIRE SPÉCIALISÉ

DATABACK
RÉCUPÉRATION DE DONNÉES

DATABACK, SOCIÉTÉ FRANÇAISE DE RÉCUPÉRATION DE DONNÉES

DATABACK, LE LEADER

DANS LA RÉCUPÉRATION ET LE TRAITEMENT DES DONNÉES SENSIBLES.

Databack est une société française spécialisée dans les services de récupération de données. Nous sommes des ingénieurs et techniciens experts dans la récupération de données depuis plus de 18 ans.

15
Collaborateurs dédiés à la récupération de données

1250
Clients sauvés par an

+ de 150
cas de rançongiciel

2
Laboratoires et salles blanches pour la R&D

18
Années d'expériences dans la récupération de données

02

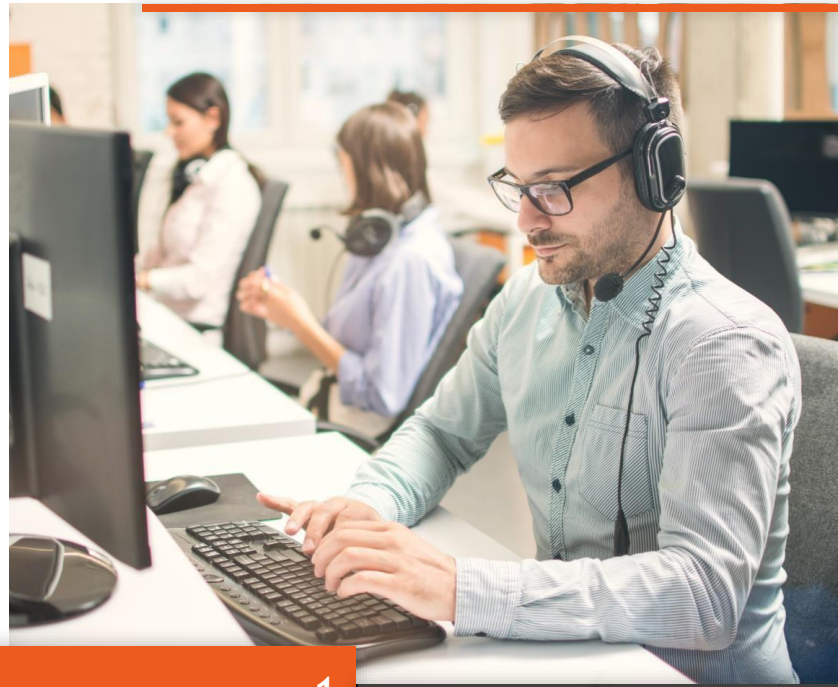
UN PROCESSUS SIMPLE, RAPIDE & SÉCURISÉ

DATABACK
RÉCUPÉRATION DE DONNÉES

FOCUS

CELLULE D'URGENCE & QUALIFICATION

Pour les cas d'extrême urgence, DATABACK a mis en place un service dédié aux récupérations de données les plus critiques.



LA CELLULE D'URGENCE C'EST

- Un numéro de téléphone dédié 24/24
- Une équipe d'astreinte disponible en moins de deux heures
- Mise en place d'un appel avec un ingénieur spécialisé
- Retour rapide de la proposition commerciale

LE PROCESSUS DATABACK, RAPIDE, SIMPLE, SÉCURISÉ

1 **CELLULE D'URGENCE ET QUALIFICATION**

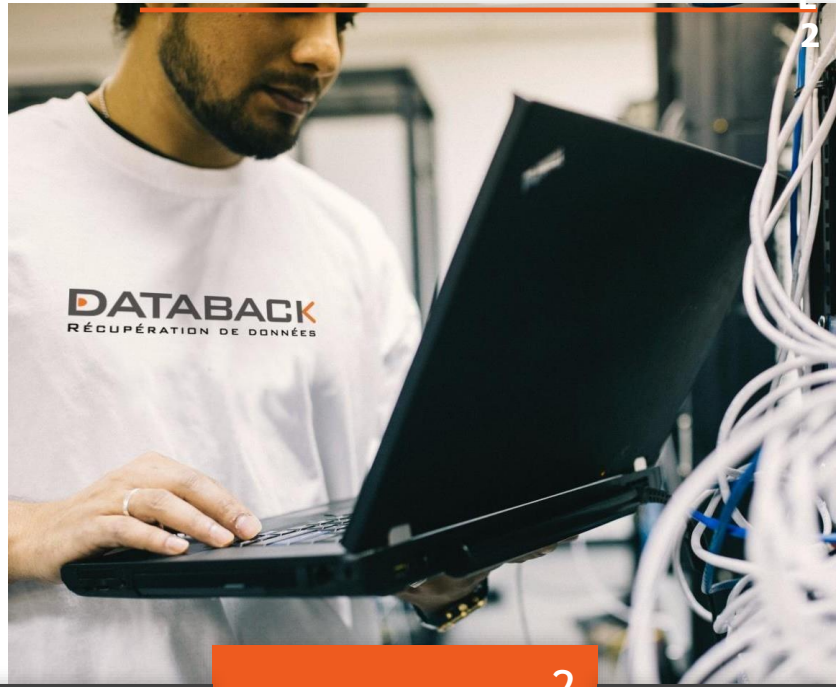
2 PRISE EN CHARGE & DIAGNOSTIC

3 ANALYSE DU CONTENU & RÉCUPÉRATION

FOCUS

PRISE EN CHARGE & DIAGNOSTIC

Databack est en mesure de récupérer les données ayant subi une attaque par rançongiciel sur tous les supports de stockage. La phase de diagnostic permet de valider la restauration des données dans le nouvel SI.



DATABACK EST SPÉCIALISÉ DANS

- Connaissance des systèmes de fichiers et des formats de sauvegarde
- Restauration des données inaccessibles suite au chiffrement
- Mise en forme pour réintégration optimisée des données chez le client

LE PROCESSUS DATABACK, RAPIDE, SIMPLE, SÉCURISÉ

1 CELLULE D'URGENCE ET QUALIFICATION

2 **PRISE EN CHARGE & DIAGNOSTIC**

3 ANALYSE DU CONTENU & RÉCUPÉRATION

FOCUS

ANALYSE DU CONTENU & RÉCUPÉRATION

Databack assure la récupération de données sur tout support de stockage utilisé par un système d'information : serveurs NAS / SAN / VSAN, baies de stockage, bandes magnétiques, disques durs et SSD

LES SERVICES DATABACK

- Récupération après chiffrement
- Migration/aide à la restauration
- Effacement sécurisé des disques infectés

LE PROCESSUS DATABACK, RAPIDE, SIMPLE, SÉCURISÉ

1 CELLULE D'URGENCE ET QUALIFICATION

2 PRISE EN CHARGE & DIAGNOSTIC

3 ANALYSE DU CONTENU & RÉCUPÉRATION

PROCESSUS DE RÉCUPÉRATION
RAPIDE ET SÉCURISÉ

1 CELLULE D'URGENCE & QUALIFACTION

Cellule d'urgence DATABACK

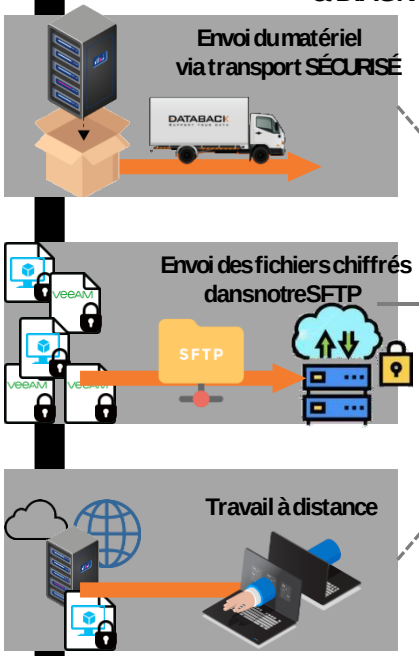
Mise en relation avec l'équipe Databack

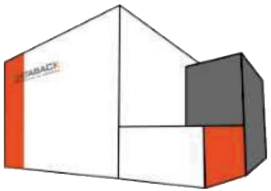
Qualification de la demande

Devis & procédure à suivre

Détection d'un matériel infecté

2 PRISE EN CHARGE & DIAGNOSTIC

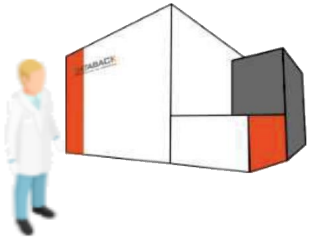




Laboratoire DATABACK

Processus de récupération des données

ANALYSE DU CONTENU & RÉCUPÉRATION



Processus de récupération

Analyse du matériel

Clonage des données

Analyse des fichiers

Restauration des données perdues

Envoi des données récupérées

DATABACK
SUPPORT YOUR DATA

03

ÉTUDE DE CAS PRATIQUE

DATABACK
SUPPORT YOUR DATA

Quelques RAPPELS…

Disque

Disque formaté

Disque formaté avec des données

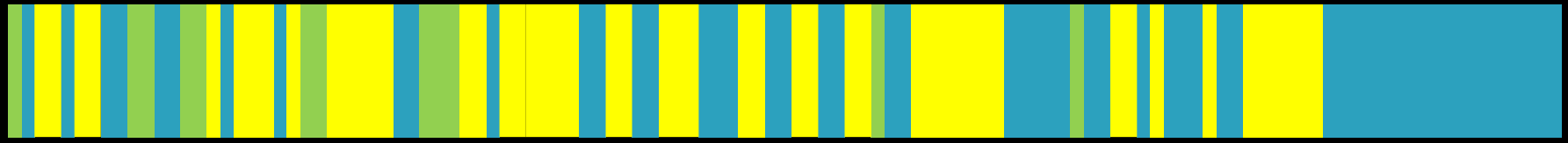
Espace libre

Metadonnées

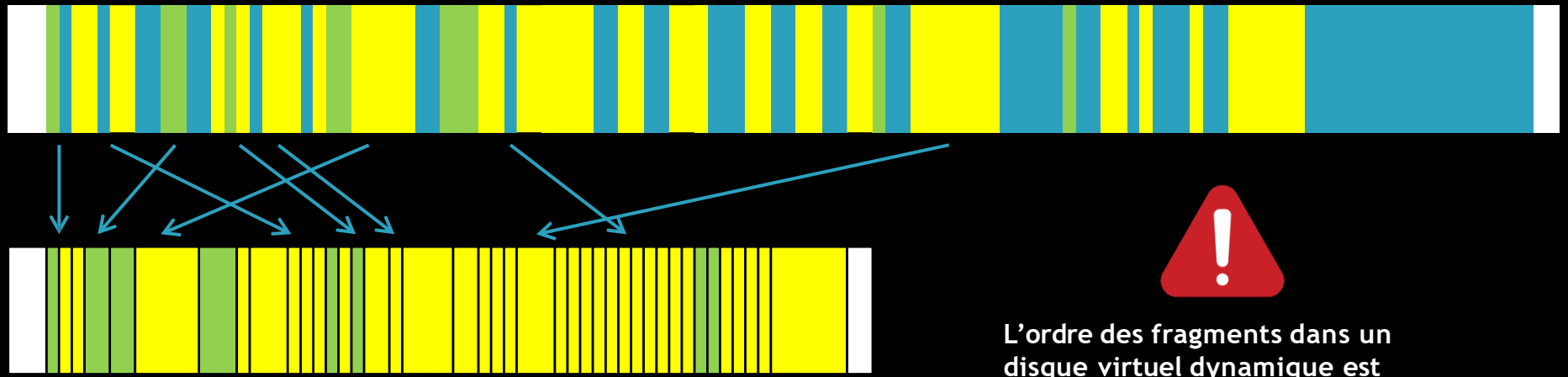
Données (fichiers)

Quelques RAPPELS…

Disque



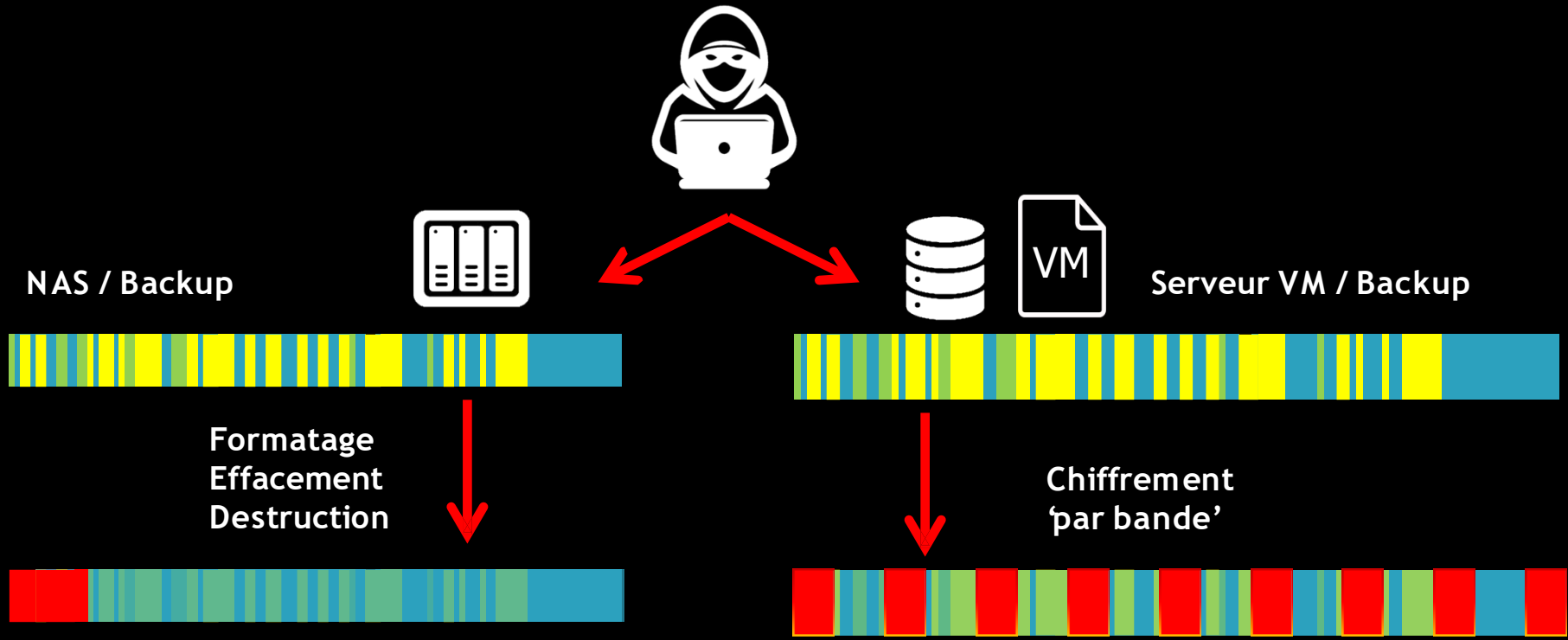
Disque virtuel (pré-alloué)



Disque virtuel (allocation dynamique)

L'ordre des fragments dans un disque virtuel dynamique est différent du disque pré-alloué

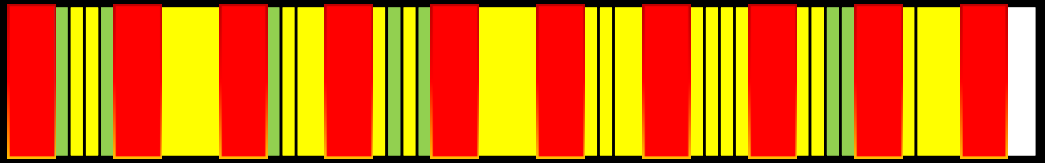
Que font les PIRATES ?



DATABACK
SUPPORT YOUR DATA

Que font les CLIENTS ?

Disque virtuel chiffré



Le chiffrement ‘par bandes’ écrase la table de translation des fragments

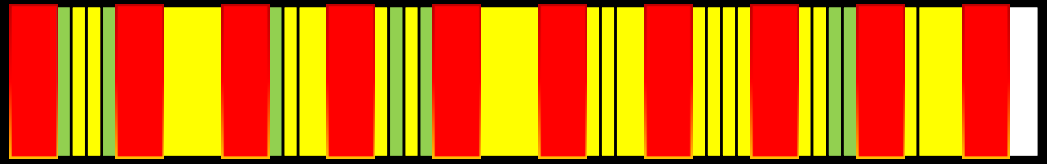
Une tentative de récupération de données avec des outils standards (ex : Photorec) :

- Récupération des fichiers avec nom, mais contenu corrompu (mauvaise allocation)

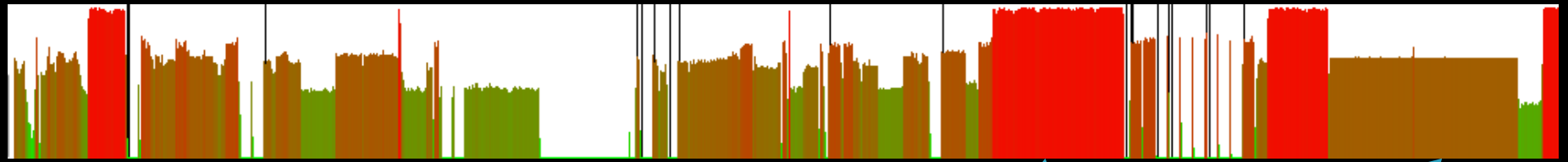
- Récupération des fichiers par signature (perte de l’arborescence et faible taux de validité des fichiers)

Que fait DATABACK ?

Disque virtuel chiffré



Nous créons une carte des zones chiffrés par analyse des zones via entropie



Zones d'entropie basse
(textes, exports xml, codes sources, …)

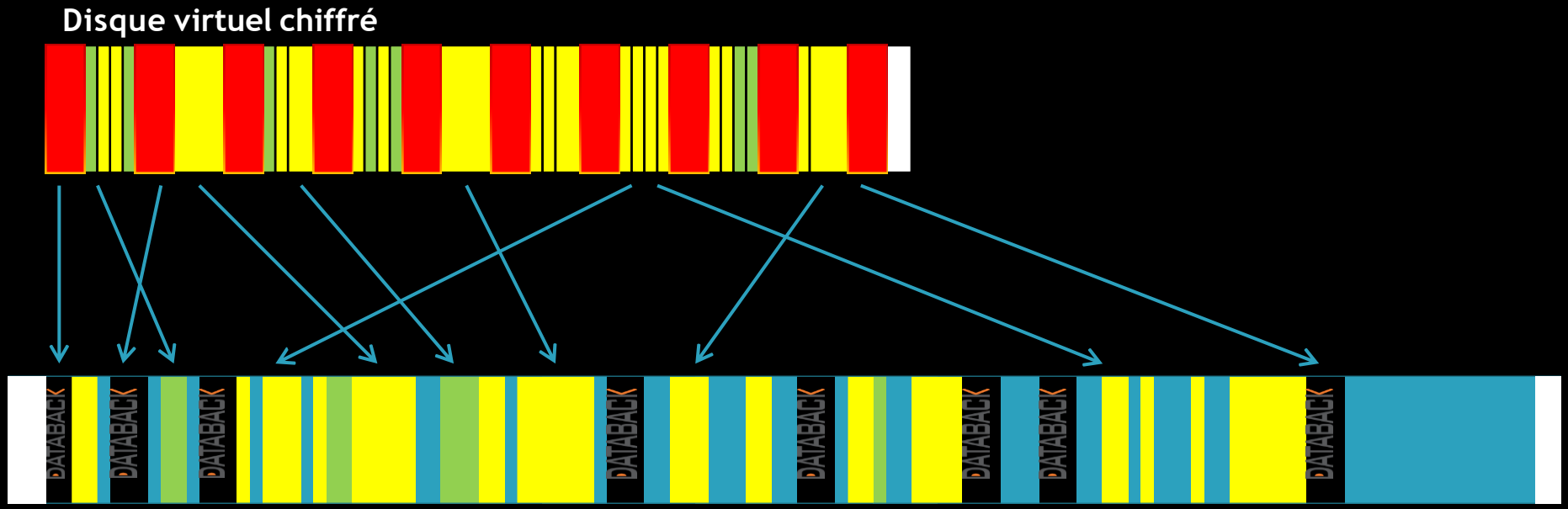
Zones d'entropie zéro
(secteurs vides ou presque vide…)

Zones d'entropie forte
(images, audios, vidéos, compressions,
ou chiffrement)

Zones d'entropie moyenne
(datas non structurées, fichiers binaires, …)

DATABACK
SUPPORT YOUR DATA

Que fait DATABACK ?



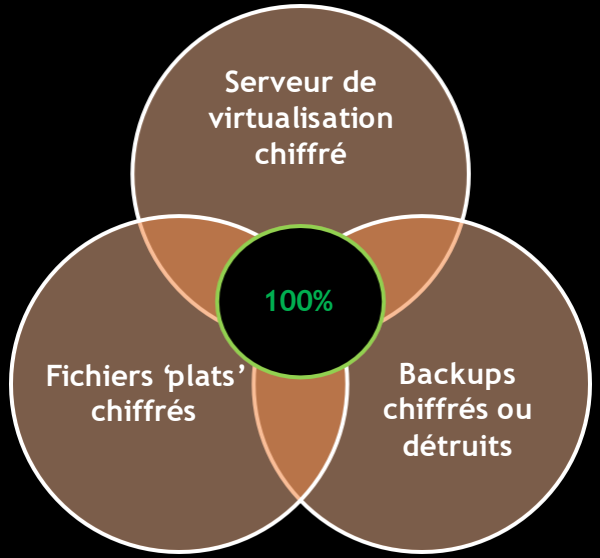
Nous reconstruisons un disque virtuel fixe. Nos analyses nous permettent de replacer tous les fragments de façon linéaire. Nous pouvons alors avoir une correspondance entre les métadonnées et les fichiers.

(Les zones noires correspondent aux zones rendues inexploitables par le chiffrement. Des marqueurs de compromissions sont insérés dans ces zones pour évaluer la validité des données).

DATABACK
SUPPORT YOUR DATA

Que fait DATABACK ?

Plus nous avons de ‘sources disponibles’
plus nous améliorons la qualité du résultat !



Que savons nous traiter ?

- Tous les *SYSTÈMES DE FICHIERS* (NTFS, Extend, BtrFS, ReFS, …)
- Toutes les *CONFIGURATIONS DE SYSTÈMES DE FICHIERS* (déduplication, versioning …)
- Tout type de *DISQUES VIRTUELS* (VMWare, Hyper-V, VirtualBox, …)
- Tous les *FORMATS DE SAUVEGARDES* (Veeam, Acronis, ActiveBackup, …)
- Tout type de *BANDES* (LTO, DAT, …)
- Tout *TYPE DE MATÉRIEL* (DELL, HP, EMC, SYNOLOGY, QNAP, …)
- Et même les *NŒUDS HYPERCONVERGÉS* (SimpliVity HPE,…)

DATABACK
SUPPORT YOUR DATA

DATABACK VOUS AIDE À ALLER PLUS LOIN :

DATABACK vous aide à :

- L’analyse forensique sur des machines corrompues ou détruites
- Réaliser des audits de vos sauvegardes pour PRA (Backup 321+)

DATABACK
SUPPORT YOUR DATA

NOUS CONTACTER

Notre équipe est à votre disposition pour répondre à toutes vos questions

24h/24 et 7J/7

Contacter l'équipe technique
ransomware@databack.fr

Numéro dédié ransomwares
02 51 31 11 65

Accès au blog professionnel
databack.fr/blog