SYNACKTIV

Un trésor dans votre grenier

Investigations à distance sur sauvegardes Veeam

FIC - Box2Box

27/03/2024

whoami

SYNACKTIV

- Maxence Fossat
- @Cybiosity 𝕏
- Analyste DFIR
- Pôle Réponse aux Incidents

CSIRT Synacktiv

SYNACKTIV

- csirt@synacktiv.com
- (+33) 9 71 18 27 69
- synacktiv.com/csirt

Plan

SYNACKTIV

- Pourquoi ce sujet ?
- Cas d'usage
- Exploration des métadonnées
- Mise en application
- Le futur

Pourquoi Veeam Backup & Replication ?

SYNACKTIV

- **Leader – Gartner® Magic Quadrant™ 7 ans d'affilée**
- **Sauvegarde / Réplication / Restauration**
- **Réponse aux Incidents**
  - Plan de Reprise d'Activité (PRA)
  - Investigations : élargissement de l'horizon temporel
- **Attaquants**
  - Cible de choix
  - Living Off the Land : chiffrement

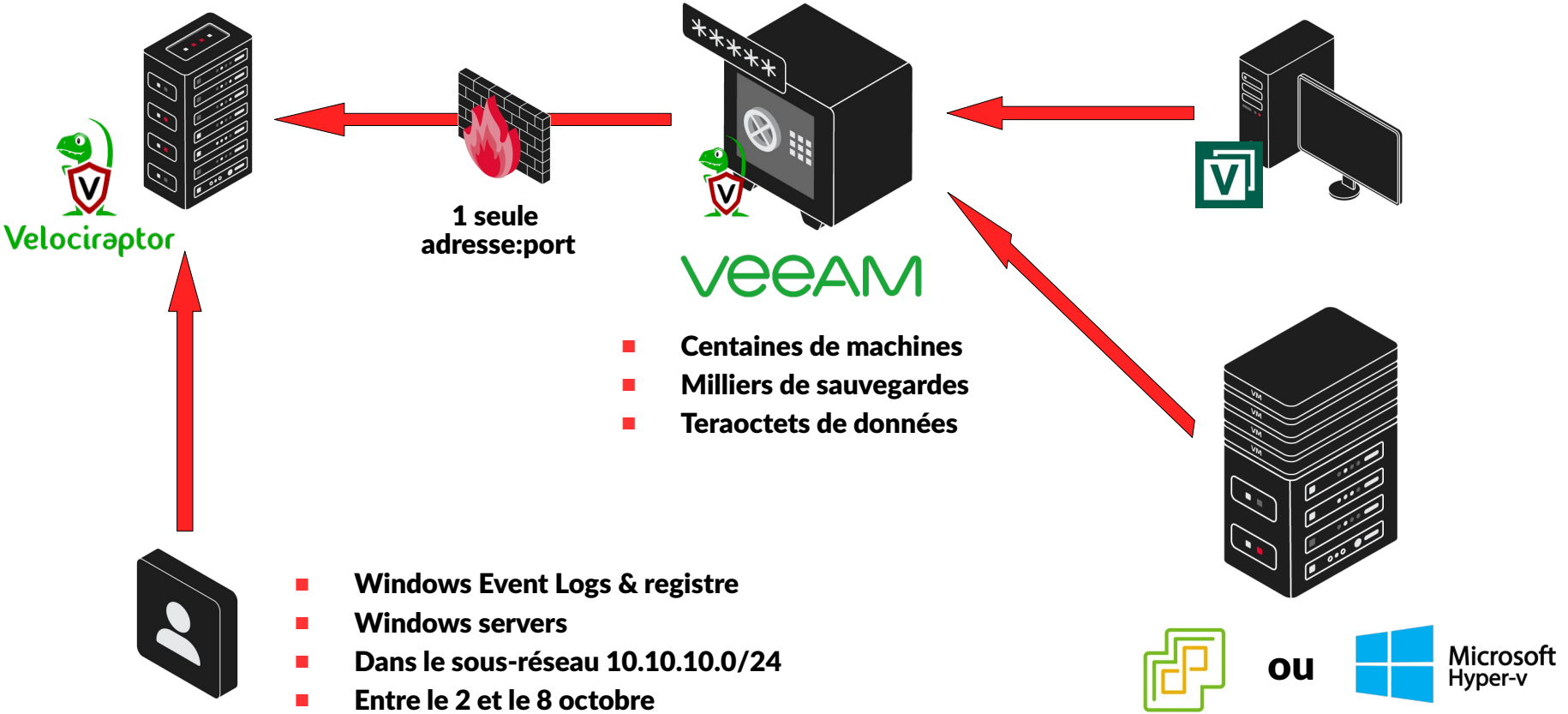
Pourquoi à distance ?

SYNACKTIV

- **Déplacement = Fait perdre du temps d'analyse**
- **Transfert de sauvegardes = Trop long, bottleneck réseau**
- **VPN = Pratique mais moins facile**

- **Ouverture de flux = Pratique (dans la plupart des cas)**
  - Ouverture vers 1 adresse:port
- **Collecte simplifiée**
  - Agent déployé sur l'ensemble du périmètre
  - Fluidité dans les échanges, moins d'aller-retours

Cas d'usage


Velociraptor
1 seule
adresse:port
VEEAM
Centaines de machines
Milliers de sauvegardes
Teraoctets de données
Windows Event Logs & registre
Windows servers
Dans le sous-réseau 10.10.10.0/24
Entre le 2 et le 8 octobre
ou
Microsoft
Hyper-v

Collecte à distance

SYNACKTIV

Avantages

- Éviter bottleneck réseau
- Répartir charge de travail
- Restreindre rapidement périmètre d'analyse

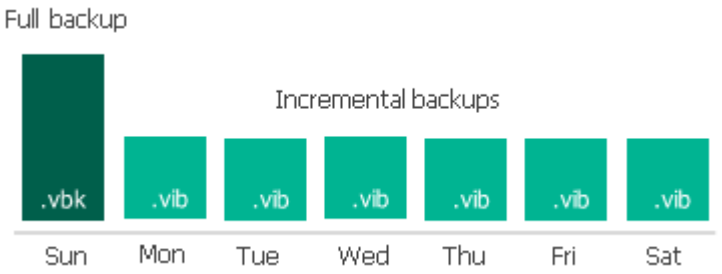
Inconvénients

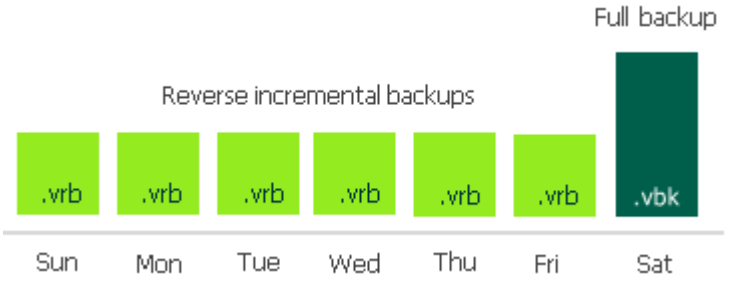
- Espace disque >= taille max sauvegarde
- Altération de la preuve

Exploration des métadonnées

Où sont elles ?

SYNACKTIV





- **Veeam backup chain metadata files : `.vbm`**
- **Veeam full backup files : `.vbk`**
- **Veeam incremental backup files : `.vib`**
- **Et aussi probablement dans :**
  - Veeam reverse incremental backup files : `.vrb`

https://helpcenter.veeam.com/docs/backup/hyperv/backup_methods.html?ver=120

Ce qu'on y trouve

SYNACKTIV

- Informations de base (hostname, adresses IP, RAM, etc.)
- Taille des disques sauvegardés
- Fichiers à extraire (`.vmdk`, `.vhdx`, etc.) + taille
- État de la sauvegarde (corrompue, etc.)
- Date de création et de complétion de la sauvegarde
- Numéro dans la chaîne

- Combiner `.vbm` et fichiers de sauvegarde

Mise en application

Trouver les sauvegardes à extraire

SYNACKTIV

- **Artifacts Velociraptor**
  - Développés par Synacktiv
  - Parsing des métadonnées

`Windows.Veeam.RestorePoints.MetadaFiles`

ou

`Windows.Veeam.RestorePoints.BackupFiles`

Trouver les sauvegardes à extraire

SYNACKTIV

DisplayName	CreationTimeUTC	CompletionTimeUTC	ApproximateSize	DisksCapacity	RestorePointNumber	RestorePointType
vsphere-windows10-vm	2024-02-29T19:07:39Z	2024-02-29T19:10:16Z	86 GB	{ "6000C29d-12ad-6758-357b-bba807f4927d" : "85899345920" }	1	Full
vsphere-windows10-vm	2024-02-29T20:11:40Z	2024-02-29T20:12:21Z	138 GB	{ "6000C291-1606-b6c4-f238-c56e318ff286" : "51539607552" "6000C29d-12ad-6758-357b-bba807f4927d" : "85899345920" }	2	Increment

Trouver les sauvegardes à extraire

SYNACKTIV

BackupFile	BackupFilePath	ExtractableFilesSize
vsphere-debian-vm.1D2024-02-29T190652_0EA1.vbk	C:\Backup\Backup Job vSphere\vsphere-debian-vm.1D2024-02-29T190652_0EA1.vbk	{ "vsphere-debian-vm.vmx" : "3621" "vsphere-debian-vm.nvram" : "8684" "vsphere-debian-vm.vmdk" : "580" "vsphere-debian-vm-flat.vmdk" : "42949672960" "FsAwareMeta:37292c59-0b37-4ee8-9c1a-805d5f2dab56:2000" : "0" }

Memory	GuestIP
2048 MiB	[0 : "fe80::ee2f:b7d1:68dd:6624" 1 : "192.168.122.214"]
1024 MiB	[0 : "fe80::215:5dff:fe7a:2301" 1 : "192.168.122.216"]

Trouver les sauvegardes à extraire

SYNACKTIV

(1) Chemin vers le fichier de sauvegarde

```
SELECT BackupFilePath (1)
  FROM source(artifact="Windows.Veeam.RestorePoints.BackupFiles")
  WHERE GuestOSName =~ 'Windows Server' (2)
  AND GuestIP =~ '10.10.10.' (3)
  AND CreationTimeUTC > '2023-10-02' AND CreationTimeUTC < '2023-10-08' (4)
```

(2) Windows Servers

(3) Dans le sous-réseau 10.10.10.0/24

(4) Entre le 2 et le 8 octobre

Extraction & Conversion

SYNACKTIV

- **Extraction de la sauvegarde**
  - Veeam Extract Utility
  - `Extract.exe -restore backup_file.vbk output\`
- **Nécessite d'être au format RAW**
- **Pour les sauvegardes Hyper-V & vSphere**
  - Conversion avec `qemu-img`
  - `qemu-img.exe convert "OUTPUT\vm-disk.vhdx" -O raw OUTPUT\dest.raw`

Triage par DFIR ORC

SYNACKTIV

- **Outil de collecte**
- **Configurable**
  - Récupération uniquement des Windows Event Logs & du registre

DFIR ORC

ANSSI

L'objectif est validé 

La suite

SYNACKTIV

- **Comprendre format `.vbk`, `.vib` (et `.vrb` ?)**
  - Récupération de sauvegardes après ransomware
- **Montage en read-only**
  - Évite la conversion au format raw
  - Permet flexibilité dans l'analyse
- **Remapping Velociraptor**
  - Lancement d'Artifacts Velociraptor directement sur image disque
  - Analyse / collecte sauvegardes Linux

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com