AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Evaluation des performances de DFIR ORC dans le cadre de son utilisation par le CERT Santé

CERT Santé

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. INTRODUCTION ET OBJET

Lors de la prise en charge d'un incident, lorsqu'une machine est soupçonnée d'être infectée, des données sont collectées afin de comprendre les actions de l'attaquant. Cette analyse permet ensuite d'orienter le choix des mesures de remédiation et de rétablir un fonctionnement normal et sécurisé. La bonne réalisation des activités d'investigation dans des délais contraints permet d'engager plus tôt la reprise d'activité. Il est donc essentiel d'optimiser la phase de collecte afin d'extraire, le plus rapidement possible, les données les plus pertinentes pour l'investigation. Il est également important de déterminer quelles données sont pertinentes à collecter, car une collecte trop large alourdit ensuite les phases de traitement et d'analyse.

Après avoir rappelé les choix de configuration de DFIR-ORC, le document présente des mesures des temps de collecte et de la taille des artefacts générés par l'outil lors de collectes dans le cadre de la prise en charge d'incidents. Elle présente également une conclusion au regard des résultats obtenus.

2. CONTEXTE DE L'EVALUATION

Pour diminuer la durée de la phase de collecte, il y a généralement deux possibilités : limiter le nombre de machines sur lesquelles on effectue les collectes ou restreindre le nombre d'artefacts à récupérer. Cette étude s'est concentrée principalement sur la seconde solution et vise à mieux estimer le coût de collecte de certains artefacts.

Pour effectuer ces collectes, le CERT Santé utilise principalement ORC. ORC [1] (Outil de Recherche de Compromission) est un outil développé par l'ANSSI pour collecter les artefacts d'un environnement Windows.

ORC a été configuré de telle sorte qu'il récupère de nombreux artefacts. Un benchmark du temps de collecte et de la taille de ces artefacts a été réalisé afin d'identifier les artefacts les plus volumineux et leur temps de collecte.

Le temps de collecte moyen et la taille moyenne de chaque artefact a été mesuré. Les moyennes de temps aident à optimiser la durée de la collecte alors que les moyennes de taille aident à optimiser la durée du traitement qui est fait par la suite.

Les mesures ont été effectuées avec une configuration d'ORC qui initialement fixe la priorité d'exécution à faible dans le but de ne pas impacter d'éventuels processus critiques de la machine. L'exécution d'ORC produit une archive qui regroupe l'ensemble des artefacts collectés de la machine.

Les mesures de temps ont été effectués sur les deux machines virtuelles ci-dessous :

Nom de la machine virtuelle	Système d'exploitation	Mémoire vive	Processeur	Espace disque Totale	Espace Disque Utilisé	Utilisation
Vm de tests	Windows 11	16 Go	Intel(R) Xeon(R) Gold 6242 CPU @ 2.80GHz (2 processeurs)	200Go	80Go	Tests
Vm de reverse	Windows 10	32 Go	Intel(R) Xeon(R) Gold 6242 CPU @ 2.80GHz (1 processeur)	800Go	180Go	Reverse

Tableau 1. Tableau descriptif des machines virtuelles

Les temps indiqués dans les logs d'exécution d'ORC (début et fin de récupération de chaque artefact) n'ont pas été utilisés, car les artefacts sont exécutés en parallèle. Des comparaisons avec des exécutions individuelles ont révélé des écarts de durée, rendant ces mesures peu fiables.

C'est pourquoi les mesures de temps ont d'abord été effectuées en exécutant ORC avec l'ensemble des artefacts, puis en retirant les artefacts un par un afin d'évaluer leur impact individuel sur la durée globale. Cette méthode de soustraction avait été initialement choisie pour que seule la collecte de l'artefact soit mesurée et que le temps de lancement d'ORC ne vienne pas parasiter les données, bien qu'il se soit finalement révélé négligeable.

ORC peut parfois se figer, puis reprendre son exécution, ainsi pour la mesure du temps de certains artefacts, plusieurs mesures ont été effectuées afin d'avoir une valeur de temps plus proche de la réalité.

Les mesures de taille ont été effectuées à partir de 30 archives issues d'incidents ainsi que les données issues de deux machines virtuelles, en relevant l'espace disque utilisé par chaque artefact.

On trouvera ci-dessous une catégorisation des principaux artefacts collectés :

- Autre : regroupe les artefacts dont la taille et le temps de collecte sont négligeables par rapport aux autres.
- Artefacts : regroupe les journaux de logiciels d'accès à distance, les journaux d'antivirus, l'historique et le cache des navigateurs, …
- ArtefactsUsers : regroupe certains scripts retrouvés dans les dossiers des utilisateurs.
- GetAutoruns / GetSamples : regroupe fichiers autoruns non signés.
- NTFSInfo [2] : regroupe les informations relatives aux systèmes de fichiers NTFS, comme les descripteurs de sécurité ou les données de la MFT.
- Spyre [3] : regroupe la liste des fichiers détectés par Spyre, le scanner d'IOC permettant, dans notre cas, d'identifier des comportements suspects dans les processus en mémoire, à l'aide de près de 100 règles Yara.
- SystemHives : regroupe les fichiers de registre Security, Software, System, Components et Default.
- Yara [4] : regroupe les fichiers détectés par la dizaine de règles cherchant des fichiers malveillants comme des documents Office ou des exécutables dans les dossiers des utilisateurs.

Les artefacts mentionnés dans la suite du document correspondent majoritairement à des catégories regroupant plusieurs artefacts.

3. RESULTATS OBTENUS ET ANALYSE

A. DUREE DE COLLECTE

Comme indiqué précédemment, les temps de collecte des artefacts suivants ont été mesurés avec ORC en priorité d'exécution faible. Des tests complémentaires ont montré que la modification de cette priorité n'avait pas d'impact significatif sur la durée de la collecte. Ce n'est pas étonnant sur des machines virtuelles car ORC est la seule tâche en cours d'exécution. Néanmoins, dans le contexte d'un incident, la collecte est souvent effectuée sur des machines préalablement isolées du réseau, dont l'activité principale est déjà diminuée. Ainsi, modifier la priorité d'ORC devrait avoir peu d'effet également sur la durée de collecte.

Voici les temps de collecte mesurés pour chaque artefact sur les deux machines virtuelles, ainsi que la moyenne des deux :

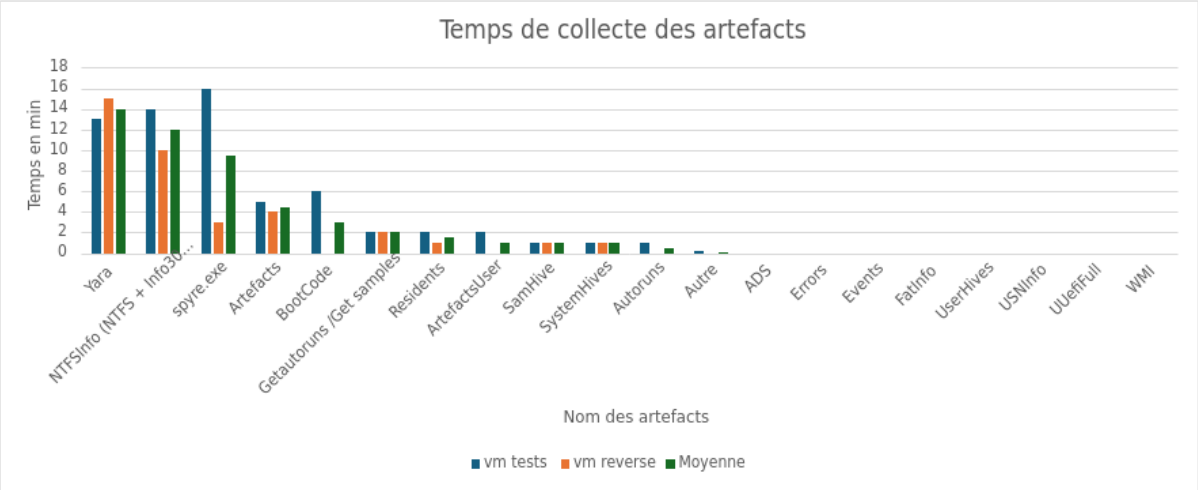


Figure 1. Histogramme du temps de collecte des artefacts

En résumé, voici les trois artefacts prenant le plus de temps à être collecté pour les deux machines virtuelles :

Numéro	Vm de tests		Vm de reverse	
	Nom	Temps en minutes	Nom	Temps en minutes
N°1	Spyre	16	Yara	15
N°2	NTFS Info	14	NTFS Info	10
N°3	Yara	13	Artefacts	4

Tableau 2. Tableau des trois artefacts les plus lents

Concernant Spyre, la collecte a duré 16 minutes sur la machine de tests et seulement 3 minutes sur la machine de reverse, cela est probablement dû au fait que la machine de reverse a plus de mémoire vive à disposition. Les deux machines virtuelles exécutent toutes les deux ORC et les processus système standards de Windows, mais la machine de reverse a 32 Go de mémoire vive alors que celle de tests en a 16 Go.

En observant que Yara, NTFSInfo et Spyre sont les éléments prenant le plus de temps à être collectés, il est possible de déterminer que ce n'est pas la collecte de fichiers qui ralentit le processus. C'est l'analyse via des règles YARA (utilisé par Yara et Spyre) et le parsing de la MFT (fait par NTFSInfo) qui sont chronophages, car ils analysent de nombreux fichiers.

B. VOLUME DE DONNEES

Voici une visualisation des données pour les tailles des artefacts sur les trente-deux archives. Cette visualisation permet de se rendre compte que les moyennes données par la suite ne sont que des indications et que des écarts de taille importants par rapport à la moyenne peuvent parfois subvenir. L'histogramme est reproduit sur une page entière en Annexe pour une meilleure lisibilité.

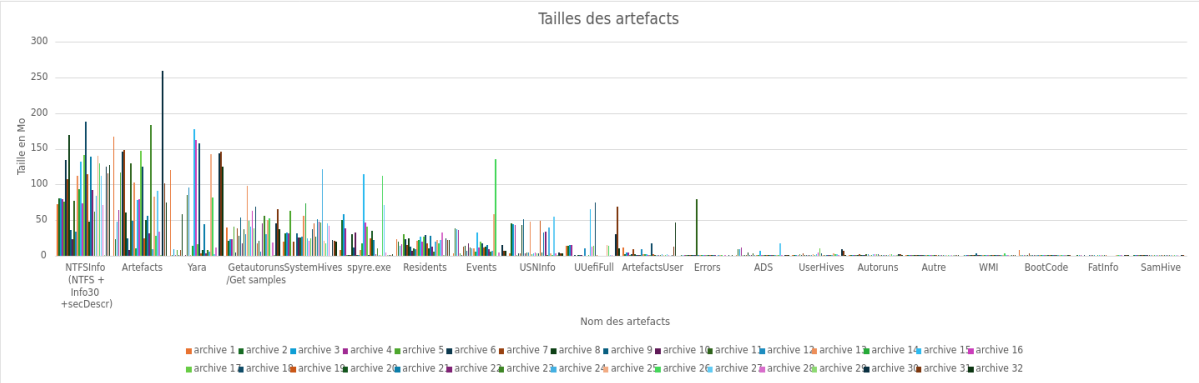


Figure 2. Histogramme des tailles des artefacts

Ci-dessous un histogramme des tailles moyennes par artefact.

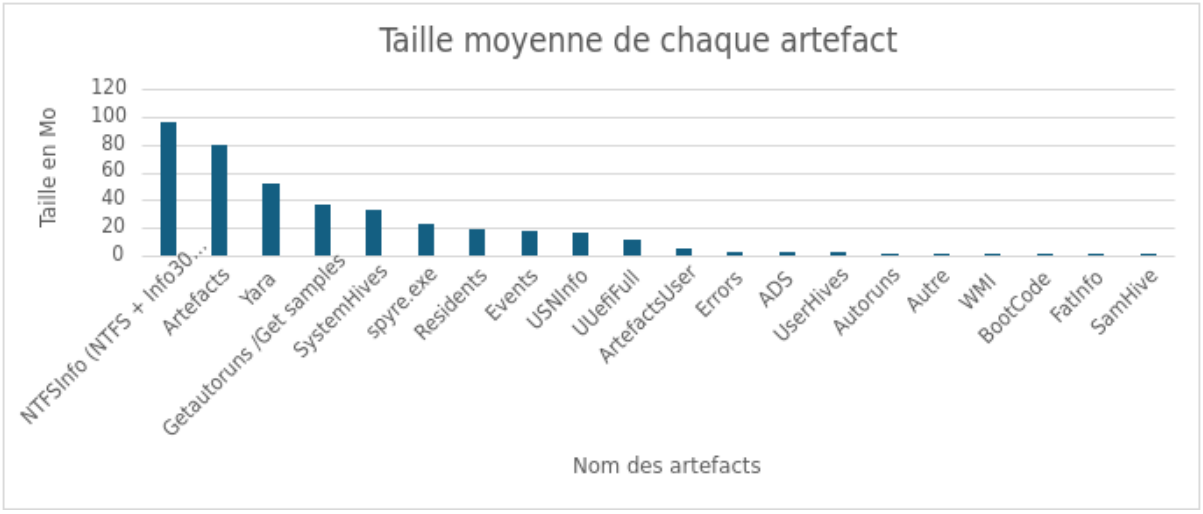


Figure 3. Histogramme des tailles moyennes des artefacts

Nous observons ainsi que NTFS Info est le plus volumineux, avec une taille moyenne de 96 Mo, puis vient Artefacts avec 80Mo et enfin Yara avec 52 Mo.

La catégorie *Artefacts* étant composée de plusieurs artefacts distincts, la répartition ci-dessous permet de mieux identifier ceux impactant le plus le volume total.

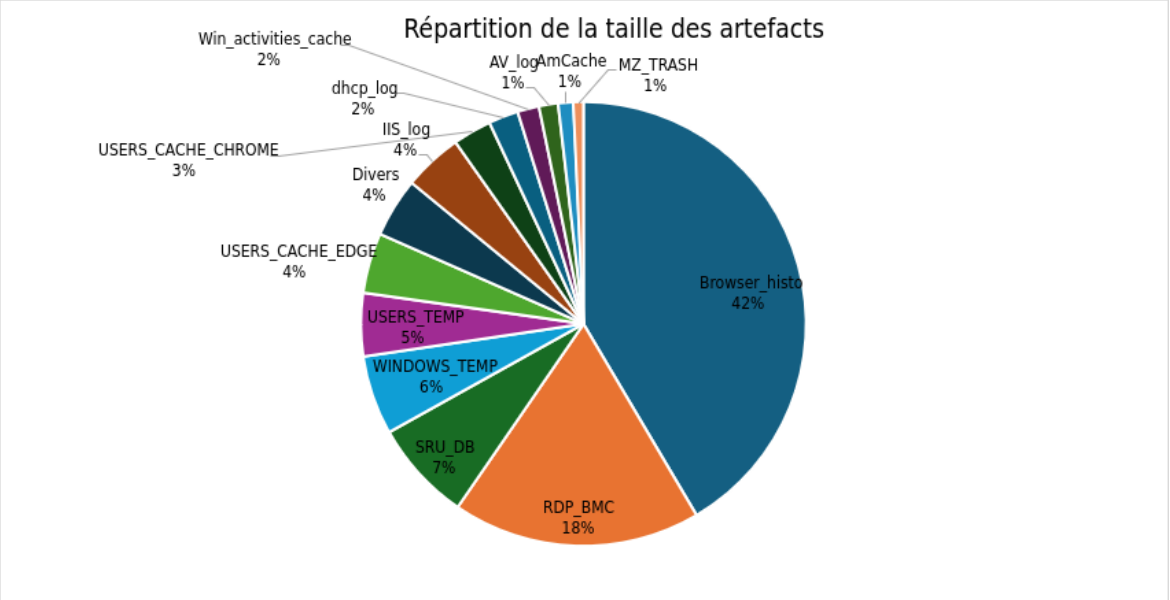


Figure 4. Diagramme circulaire de la répartition de taille des artefacts

Le tableau ci-après représente les trois types de données qui occupent le plus d'espace :

Numéro	Données récupérées	Pourcentage	Noms des artefacts
1	Historique et cache du navigateur	49%	browser_histo + USERS_CACHE_EDGE + USERS_CACHE_CHROME
2	Cache RDP	18%	RDP_BMC
3	Fichiers des dossiers temporaires	11%	WINDOWS_TEMP + USERS_TEMP

Tableau 3. Tableau des trois artefacts les plus volumineux de la catégorie Artefact

Les données de navigation (historique, cache) permettent d'identifier les sites consultés ou les fichiers potentiellement téléchargés, ce qui est utile en cas de suspicion de phishing ou de téléchargement de malware via un navigateur. Le cache RDP contient des fragments de l'écran de la machine lors des sessions. Ainsi, il peut être utile pour voir ce qu'a fait l'attaquant, s'il s'est connecté en RDP. Les dossiers temporaires peuvent permettre de retrouver des exécutables ou scripts utilisés par l'attaquant.

En séparant les données de taille par type de machine, comme le montre l'histogramme ci-dessous, on remarque que, pour Yara, seuls les postes de travail fournissent des volumes importants. Ainsi, le troisième pour les serveurs et contrôleurs de domaine serait plutôt Getautoruns/Getsamples qui regroupe les fichiers autoruns non signés.

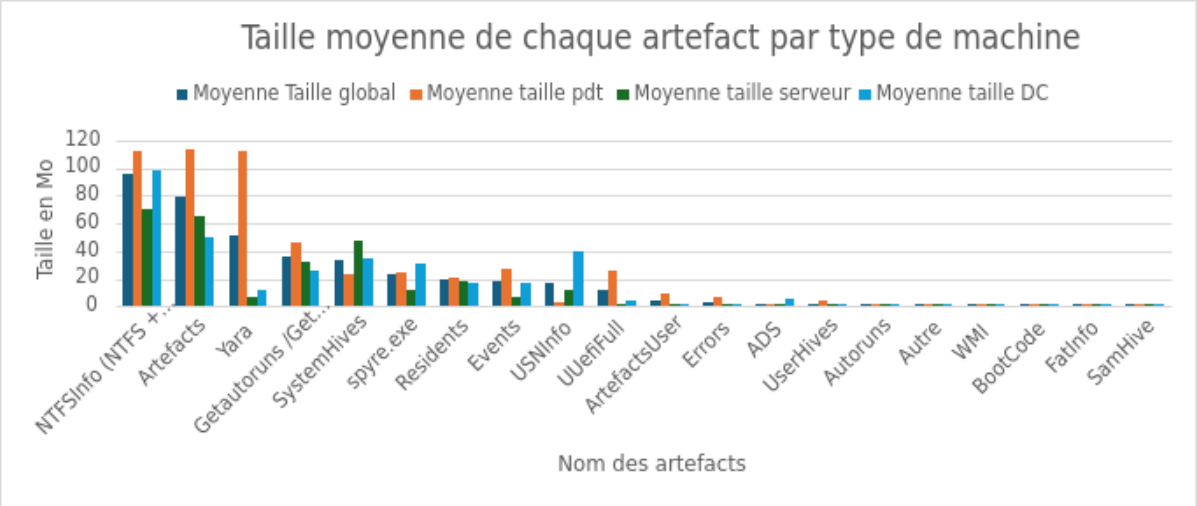


Figure 5. Histogramme des tailles moyennes par type de machine

4. PRESENTATION DES RESULTATS SUR LES DEUX DIMENSIONS

Finalement, voici un graphe permettant d'identifier plus facilement les artefacts couteux en temps, ceux couteux en taille et ceux couteux en taille et en temps.

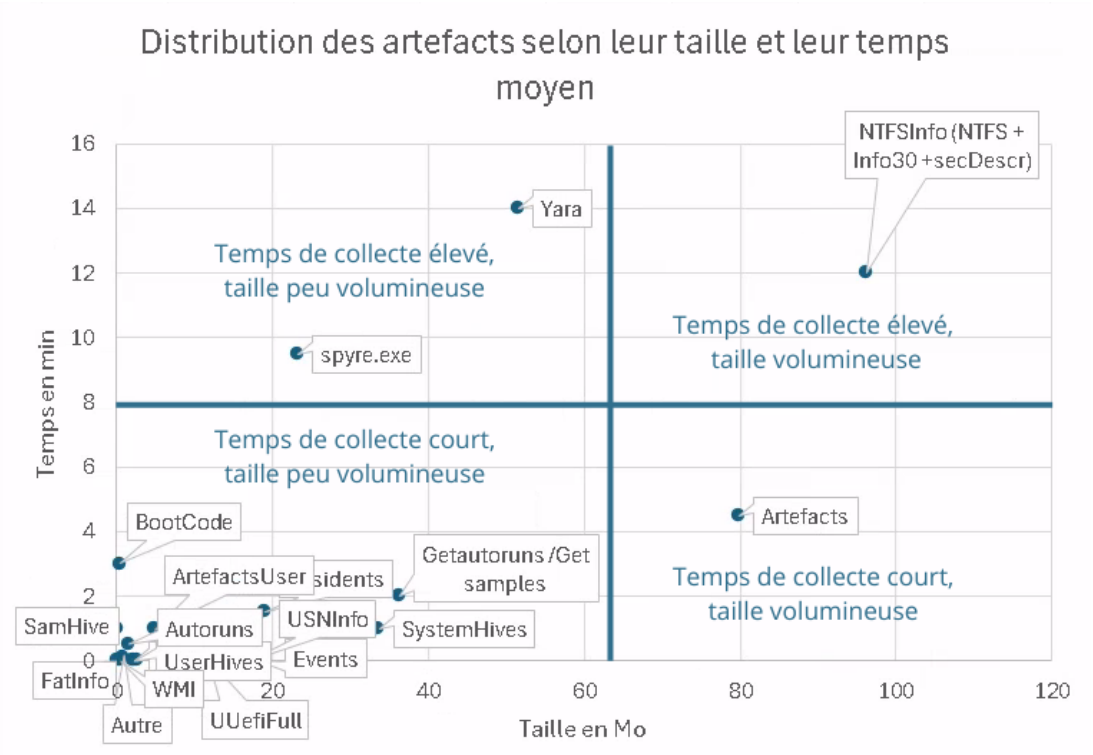


Figure 6. Distribution des artefacts selon leur taille et leur temps moyen

Le schéma final montre qu'un temps de collecte élevé n'implique pas nécessairement un artefact volumineux, comme le montrent Spyre et Yara. Et qu'à l'inverse des artefacts volumineux, comme ceux de la catégorie Artefacts, peuvent être récupérés rapidement. Ainsi, le temps de collecte est principalement affecté par l'évaluation des fichiers pour faire correspondre des règles à la recherche de fichiers sur le disque, plutôt qu'à la récupération proprement dite des fichiers.

La séparation de ce graphe en quatre zones permet de mieux distinguer les différents cas de figure.

La case en bas à droite représente les artefacts alourdissant la collecte en taille, mais pas en temps. Ainsi, les analystes avec des infrastructures importantes peuvent se permettre de récupérer ces artefacts, mais les plus petits devront faire le tri et évaluer la pertinence de récupérer les données de navigateurs ou les données d'utilisateurs.

Les artefacts en haut à gauche impactent principalement le temps de collecte. Ainsi, pour réduire ce temps, il faut réfléchir sur leur utilité. Comme Spyre et Yara se basent tous les deux sur des règles Yara, il peut être intéressant de réduire le nombre de règles afin de réduire le temps de collecte. Mais si les données ne sont pas analysées par la suite, alors il sera plus intéressant de ne pas les récupérer en premier lieu.

Les artefacts en bas à gauche peuvent être récupérés de manière systématique, car ils n'impactent pas significativement la taille de l'archive ou le temps de collecte.

Enfin, l'artefact situé en haut à droite, NTFSInfo, est coûteux à la fois en taille et en temps de collecte, mais il reste très souvent indispensable.

Pour les analystes disposant d'infrastructures capables de stocker et traiter de grands volumes de données, il est possible de collecter de nombreux artefacts et de les analyser a posteriori. À l'inverse, dans le cas d'infrastructures plus limitées, il est préférable de s'appuyer sur des règles Yara pour filtrer en amont les données pertinentes.

5. CONCLUSION

Les artefacts prenant le plus de temps à être collectés sont NTFSInfo, Spyre et Yara car ils réalisent des prétraitements ou des analyses de nombreux fichiers. Et concernant la taille, les plus couteux sont NTFSInfo et Artefacts. NTFS contient la liste de tous les fichiers de la machine et Artefacts contient les données des navigateurs qui sont volumineuses.

On peut donc en déduire que les méthodes de prétraitement ou de sélection de l'information ralentissent significativement la collecte ORC. Récupérer une quantité importante de données ne signifie pas que cela prendra beaucoup de temps.

Cette étude constitue une première base pour estimer la taille et le temps de collecte moyen des artefacts, mais elle pourrait être approfondie par des mesures complémentaires.

Pour confirmer la validité des données de temps, il serait pertinent de les effectuer sur d'autres environnements, comme des serveurs ou des contrôleurs de domaine, mais aussi sur des postes de travail dotés des applications couramment utilisées pour répliquer des environnements plus réalistes. Cela permettrait d'obtenir des résultats plus proches des conditions réelles et applicables à différents types d'environnements.

De plus, il pourrait être intéressant de voir l'impact du nombre de règles Yara sur le temps de collecte de Yara ou Spyre. Dans notre cas, nous avons effectué la collecte Yara en utilisant une dizaine de règles. Il serait intéressant de connaître le temps nécessaire à la collecte avec 30 ou 50 règles.

6. REFERENCES

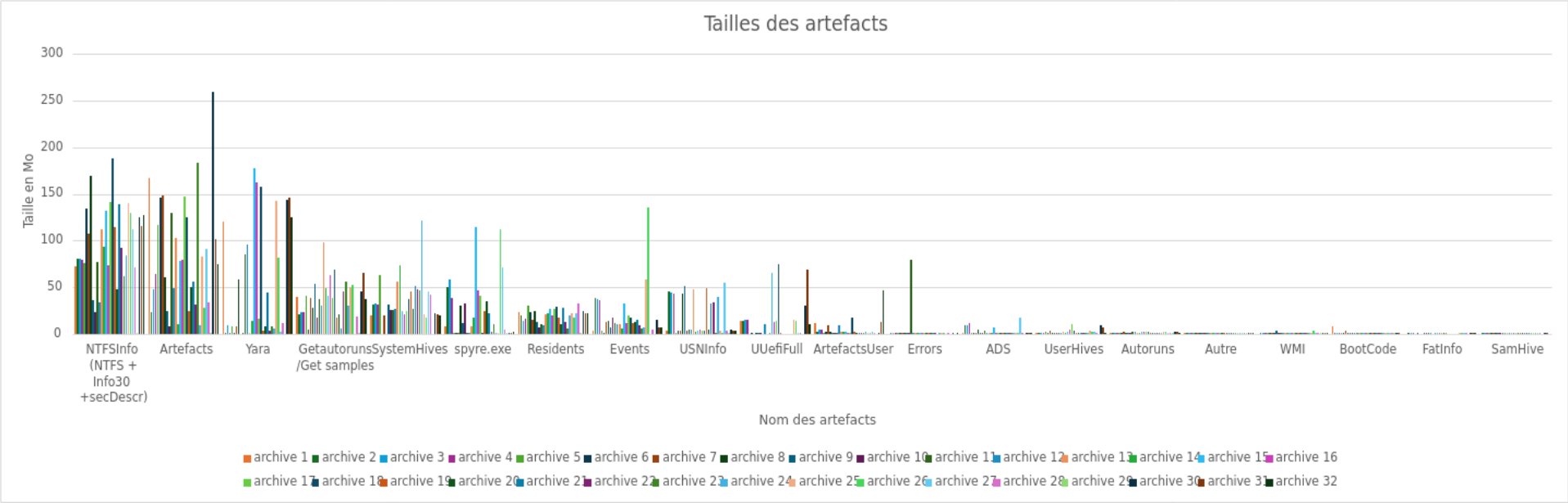
[1] «GitHub DFIR ORC,» [En ligne]. Available: https://github.com/DFIR-ORC/dfir-orc.

[2] ANSSI, [En ligne]. Available: https://dfir-orc.github.io/NTFSInfo.html.

[3] «Github de Spyre,» [En ligne]. Available: https://github.com/spyre-project/spyre.

[4] ANSSI, [En ligne]. Available: https://dfir-orc.github.io/configuring_yara.html.

7. ANNEXE


Tailles des artefacts
Taille en Mo
300
250
200
150
100
50
0
NTFSInfo (NTFS + Info30 +secDescr)
Artefacts
Yara
GetautorunsSystemHives /Get samples
spyre.exe
Residents
Events
USNInfo
UUefiFull
ArtefactsUser
Errors
ADS
UserHives
Autoruns
Autre
WMI
BootCode
FatInfo
SamHive
Nom des artefacts
archive 1 archive 2 archive 3 archive 4 archive 5 archive 6 archive 7 archive 8 archive 9 archive 10 archive 11 archive 12 archive 13 archive 14 archive 15 archive 16
archive 17 archive 18 archive 19 archive 20 archive 21 archive 22 archive 23 archive 24 archive 25 archive 26 archive 27 archive 28 archive 29 archive 30 archive 31 archive 32