Centralisation et optimisation de l'analyse mémoire

-

Investigation numérique et réponse à incidents

Félix Guyard

0 – Présentation

Forensic X Lab

ForensicXlab

- Recherche
- Partages de ressources et de connaissances à la communauté
- Collaboration avec un expert judiciaire.

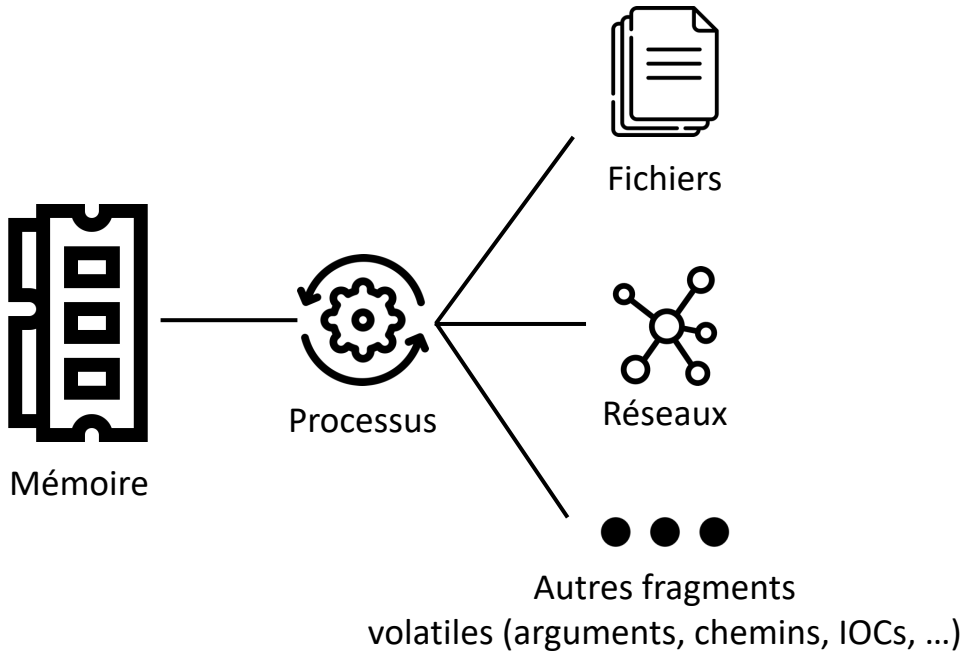
0 - Agenda

- Introduction
- Problématiques
- Volatility3 et VolWeb
- Cas d’usage
- Démonstration
- Conclusion

1 – Introduction

L'analyse mémoire :

Extraction d'artefacts via l'exploitation de la mémoire volatile RAM (Random Access Memory).



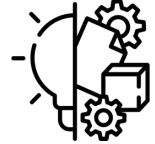
Avantages :

- Fragments mémoire volatiles uniques
- Profilage
- Meilleur contexte machine
- Contournement de certaines techniques d'obfuscation et anti-forensique.

Inconvénients :

- Fragments facilement perdus
- Obtention de l'image mémoire
- Reconstruction du contexte mémoire.

2 – Volatility3



Actuellement un des meilleurs outils d'analyse mémoire avec un communauté très active.

La Volatility Foundation a publié une refonte complète du framework nommé Volatility3.

En cours de développement actif (version 2.5.2 actuellement)

```
~/work/DFIR/Memory_Forensics/Tools/VolWeb (main) » vol -f s3://1927cb7b-c8d6-4252-b1a2-f9168182a51d/Investigation-2.raw windows.pstree
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0x823c8830      51      244     N/A     False   N/A     N/A
* 348   4       smss.exe        0x82169020      3       19      N/A     False   2017-05-12 21:21:55.000000      N/A
** 620  348     winlogon.exe    0x8216e020      23      536     0       False   2017-05-12 21:22:01.000000      N/A
*** 664 620     services.exe    0x821937f0      15      265     0       False   2017-05-12 21:22:01.000000      N/A
**** 1024       664     svchost.exe     0x821af7e8      79      1366    0       False   2017-05-12 21:22:03.000000      N/A
***** 1768      1024    wuauclt.exe     0x81f747c0      7       132     0       False   2017-05-12 21:22:52.000000      N/A
***** 1168      1024    wscntfy.exe     0x81fea8a0      1       37      0       False   2017-05-12 21:22:56.000000      N/A
**** 1152       664     svchost.exe     0x821bea78      10      173     0       False   2017-05-12 21:22:06.000000      N/A
**** 544        664     alg.exe 0x82010020      6       101     0       False   2017-05-12 21:22:55.000000      N/A
**** 836        664     svchost.exe     0x8221a2c0      19      211     0       False   2017-05-12 21:22:02.000000      N/A
**** 260        664     svchost.exe     0x81fb95d8      5       105     0       False   2017-05-12 21:22:18.000000      N/A
**** 904        664     svchost.exe     0x821b5230      9       227     0       False   2017-05-12 21:22:03.000000      N/A
**** 1484       664     spoolsv.exe     0x821e2da0      14      124     0       False   2017-05-12 21:22:09.000000      N/A
**** 1084       664     svchost.exe     0x8203b7a8      6       72      0       False   2017-05-12 21:22:03.000000      N/A
*** 676 620     lsass.exe       0x82191658      23      353     0       False   2017-05-12 21:22:01.000000      N/A
** 596  348     csrss.exe       0x82161da0      12      352     0       False   2017-05-12 21:22:00.000000      N/A
1636    1608    explorer.exe    0x821d9da0      11      331     0       False   2017-05-12 21:22:10.000000      N/A
* 1956  1636    ctfmon.exe      0x82231da0      1       86      0       False   2017-05-12 21:22:14.000000      N/A
* 1940  1636    taskshe.exe     0x82218da0      7       51      0       False   2017-05-12 21:22:14.000000      N/A
** 740  1940    @WanaDecryptor@ 0x81fde308      2       70      0       False   2017-05-12 21:22:22.000000      N/A
(venv)
```

Sortie standard volatility3

Problématiques:

Centralisation de l'investigation et des images

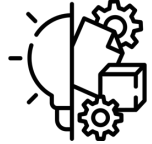
Collaboration

Visualisation

Actions répétitives

Communication DFIR/CTI

3 – VolWeb

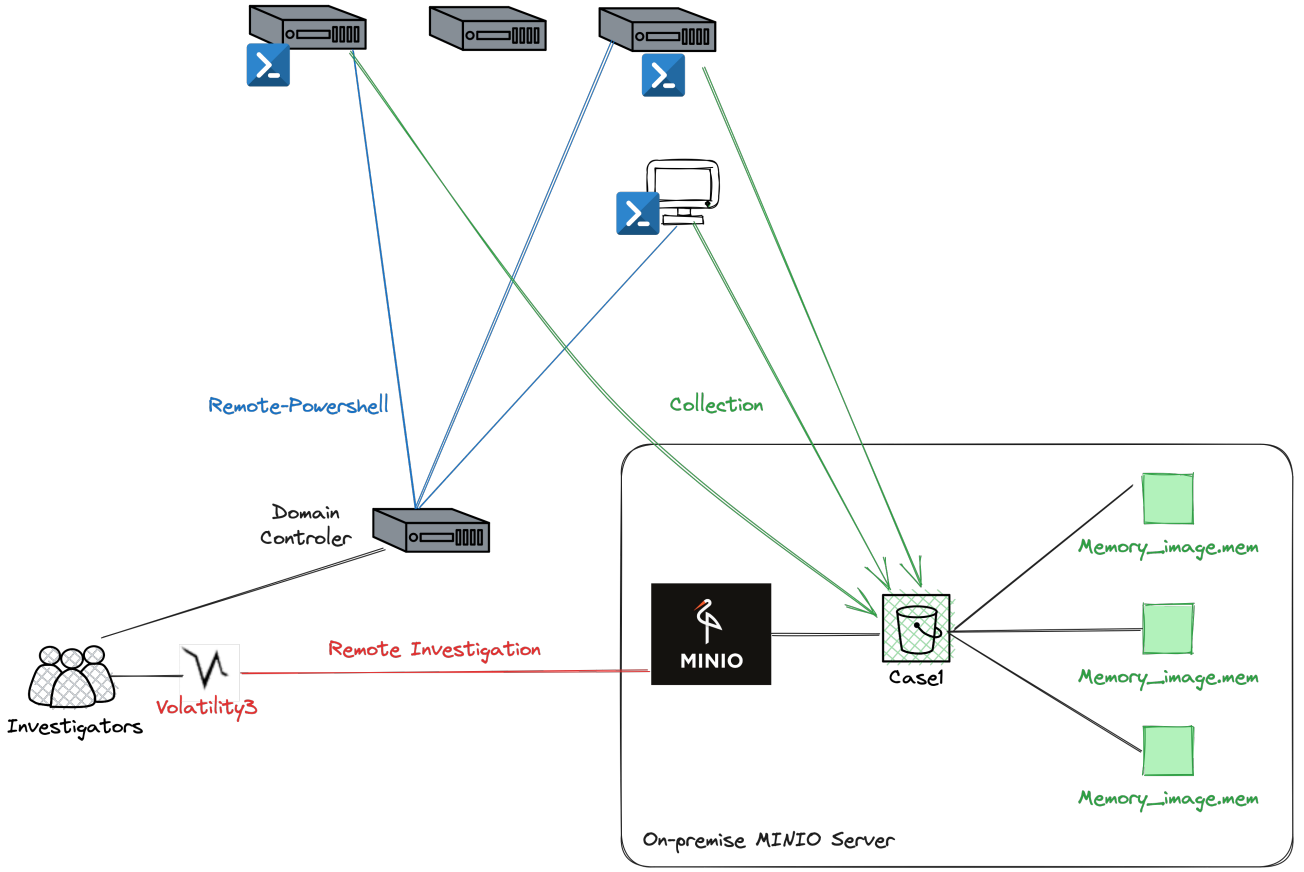


VolWeb

- Centralise vos images mémoire depuis n’importe quelles sources.
- Flexible selon les besoins
- Centralise le processus d’analyse via les moteurs d’extraction via l’utilisation de volatility3 en tant que bibliothèque.
- Permet l’analyse via des outils de visualisations uniques.
- Accélère le partage d'indicateurs.
- Interaction forte avec l'analyste via le scripting.

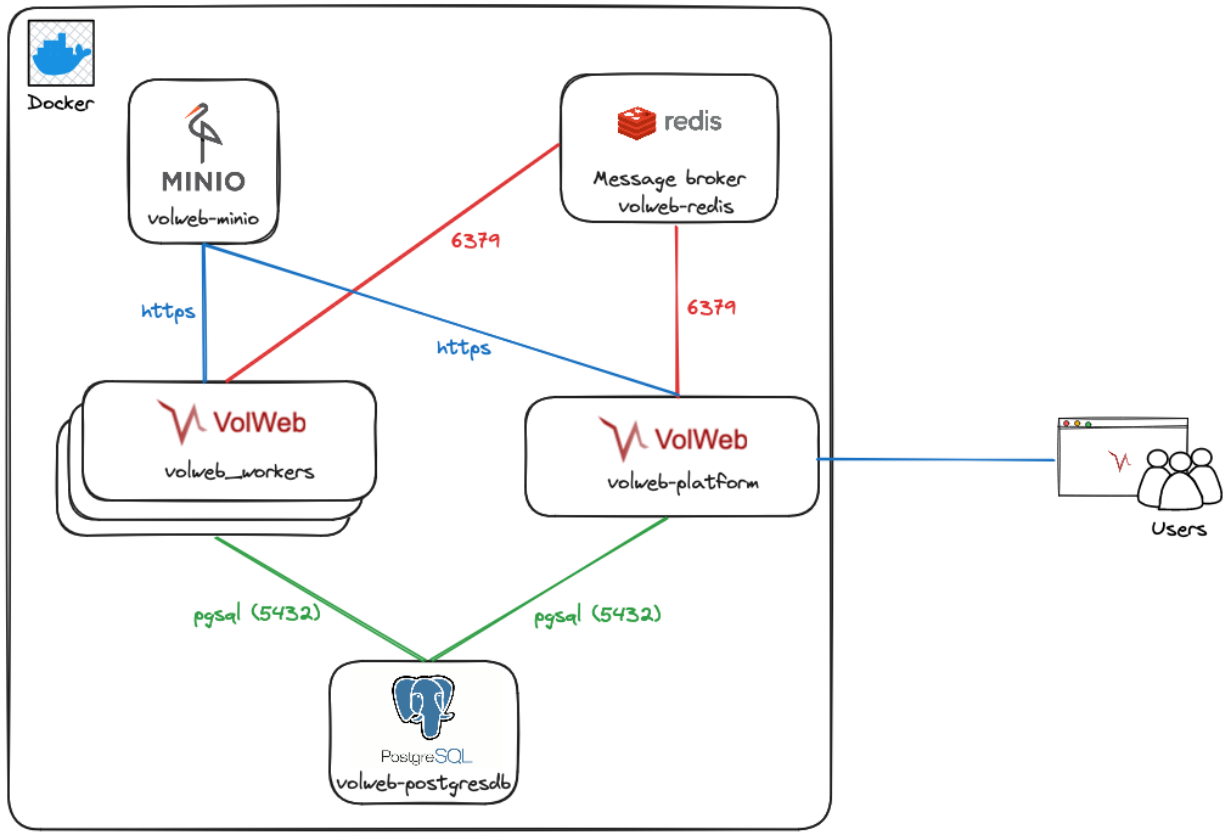
4 – Problématique: L'analyse mémoire sur le stockage objet

L'idée: Permettre l'analyse mémoire sur le stockage objet.



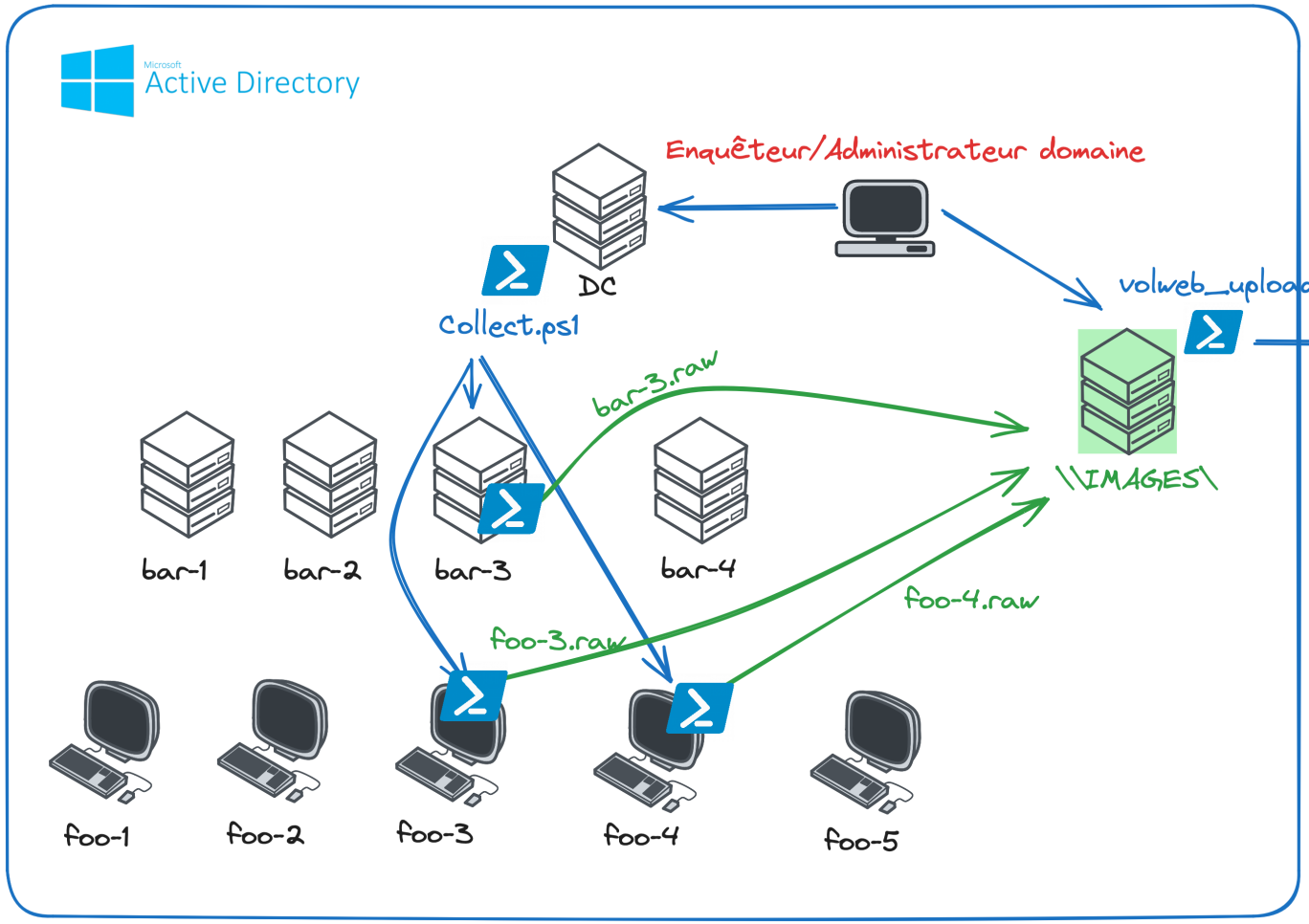
- Création de la couche de traduction volatility3 pour le support d'analyse d'une image mémoire stocké sur les technologies S3 et stockage gcloud: https://www.forensicxlab.com/posts/vols3/
- Fonctionnalité incluse dans volatility3 depuis la version 2.5.2 (décembre 2023)

5 – Technologies



- Stockage objet on-premise ou déporté
- Base de données pour le stockage et interrogation des artefacts.
- API REST exposée pour les analystes
- Worker(s) pour le traitement de l'analyse
- Redis pour la file de messages et la gestion des channels.

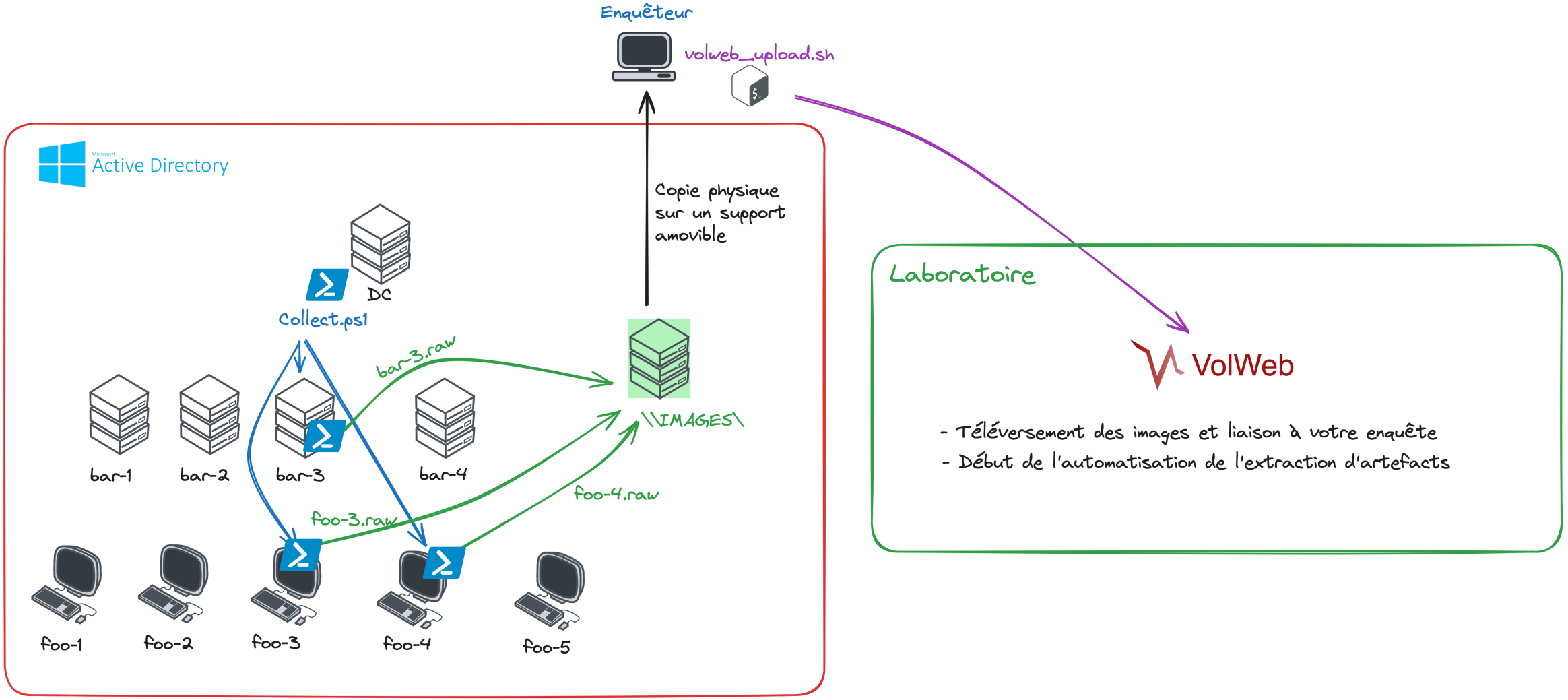
6.0 – Les possibilités: Recherche de compromission.



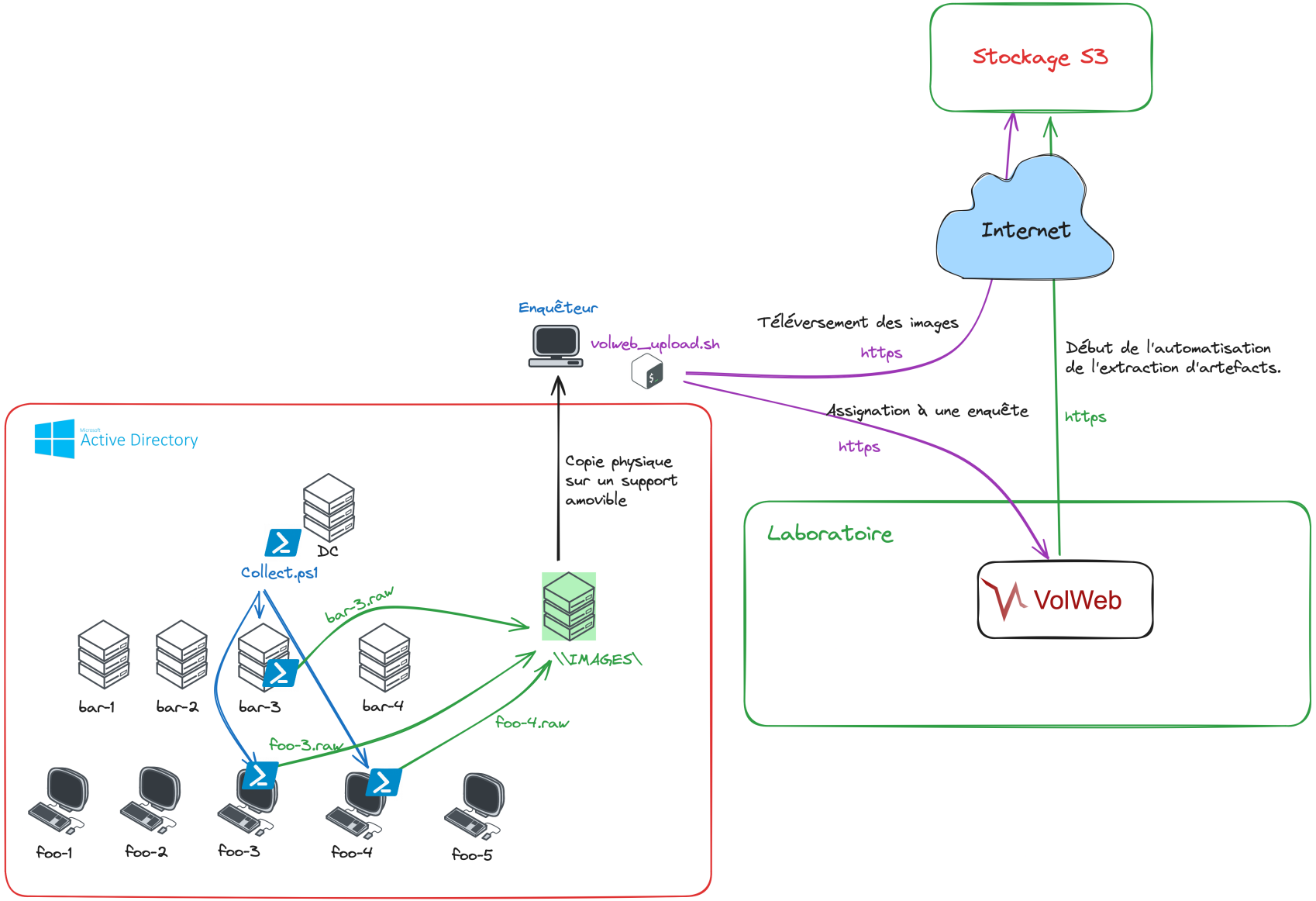
VolWeb

- Téléversement des images et liaison à votre enquête
- Début de l'automatisation de l'extraction d'artefacts

6.1 – Les possibilités: Réponse à incidents/Réquisitions.



6.2 – Les possibilités: Stockage objet déporté.



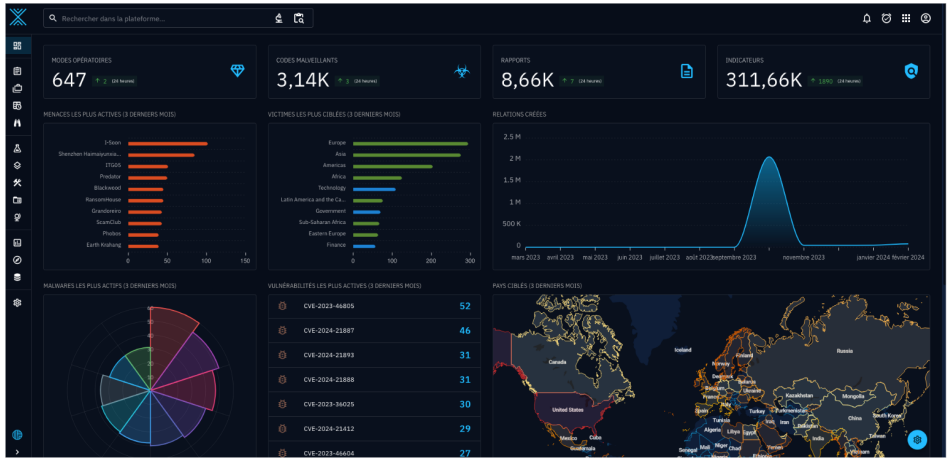
6.3 – Les possibilités: Interaction forte avec l'équipe CTI

VolWeb

Enquêter et identifier des marqueurs de compromission

Bundle STIX

OpenCTI



Importer, Qualifier et actionner les marqueurs

7 – Démonstration

8 – Conclusion

VolWeb ne remplace pas Volatility3

Les projets liés à VolWeb:

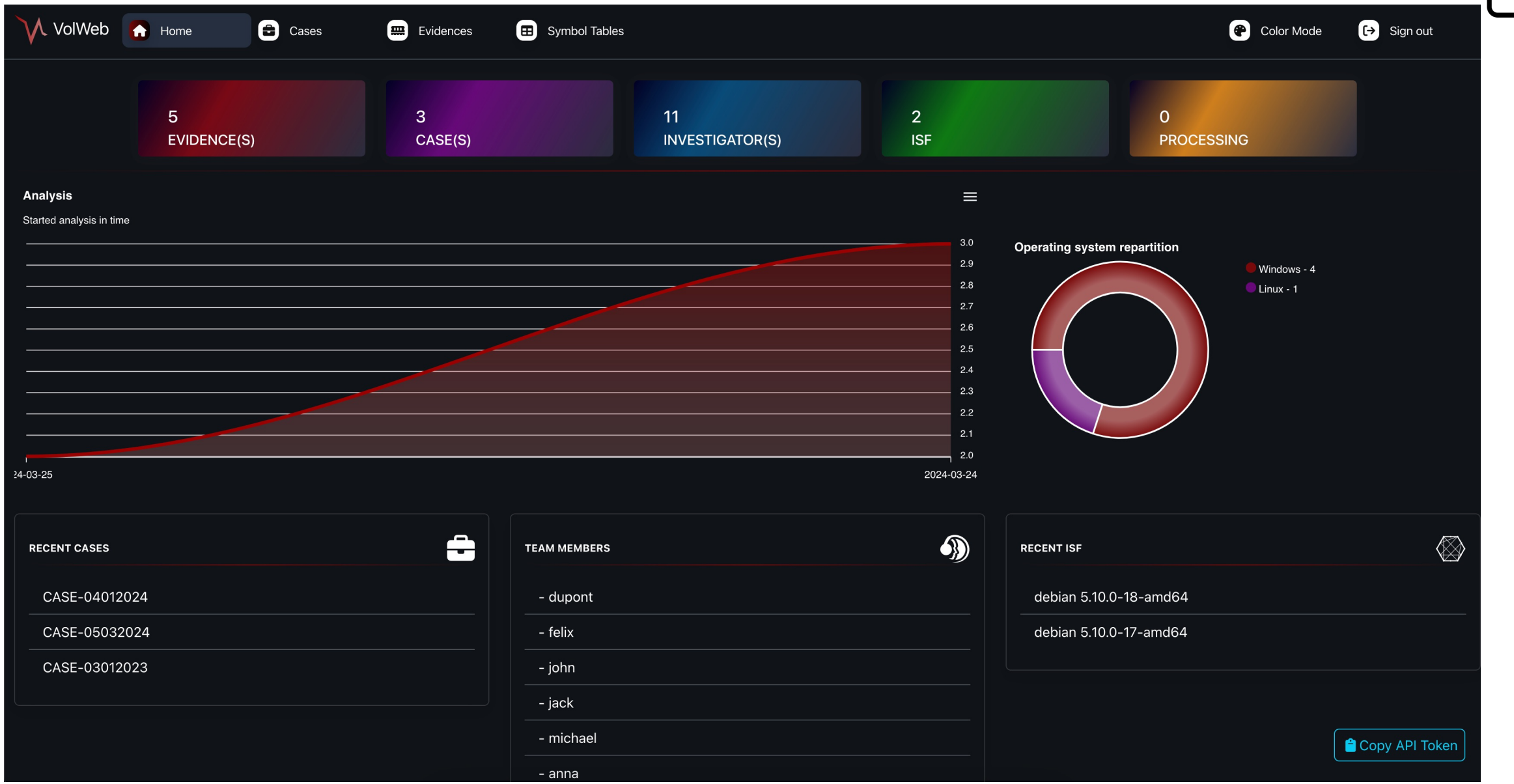
- https://github.com/k1nd0ne/VolWeb --> Plateforme (déploiement, tutoriels, documentation)
- https://github.com/forensicxlab/VolWeb-Scripts --> Scripts pour les interactions avec VolWeb.
- https://github.com/volatilityfoundation/volatility3 --> Framework volatility3

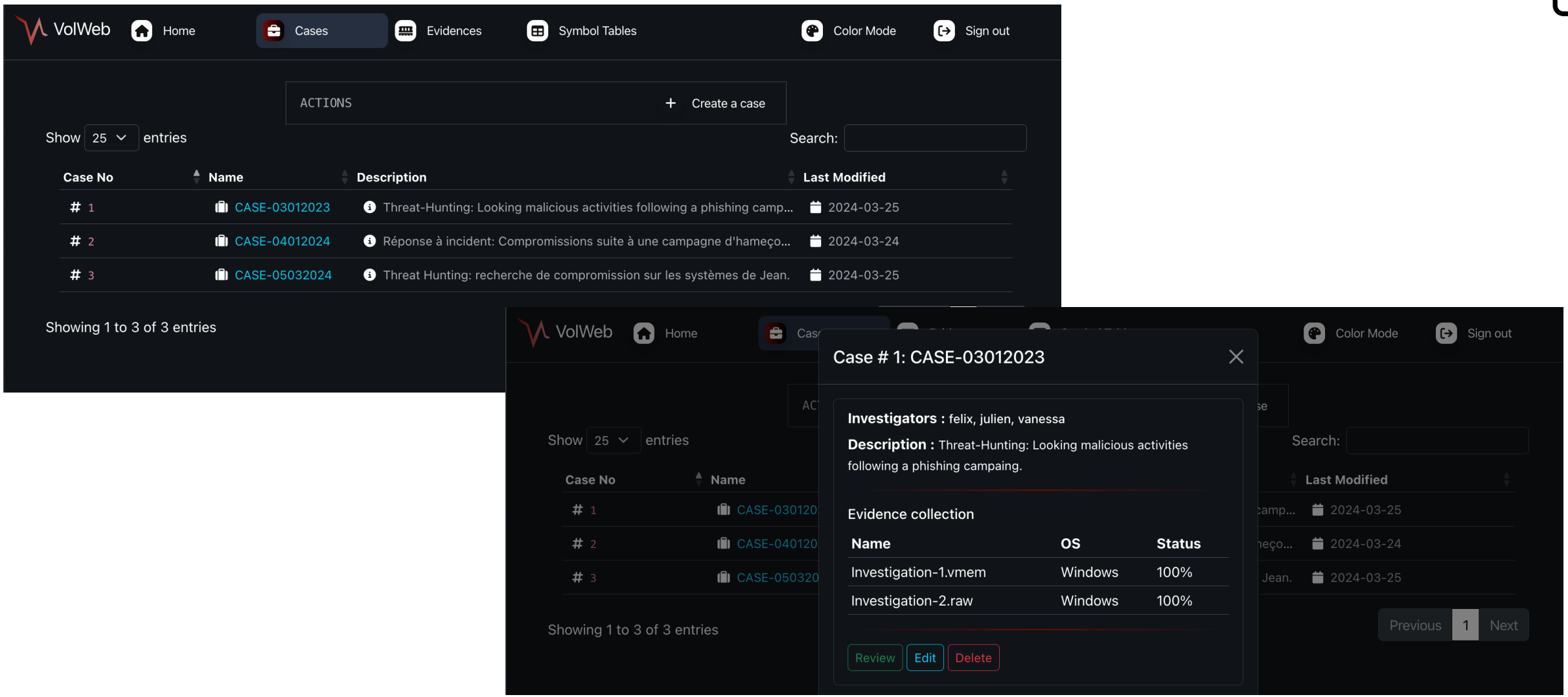
Les objectifs:

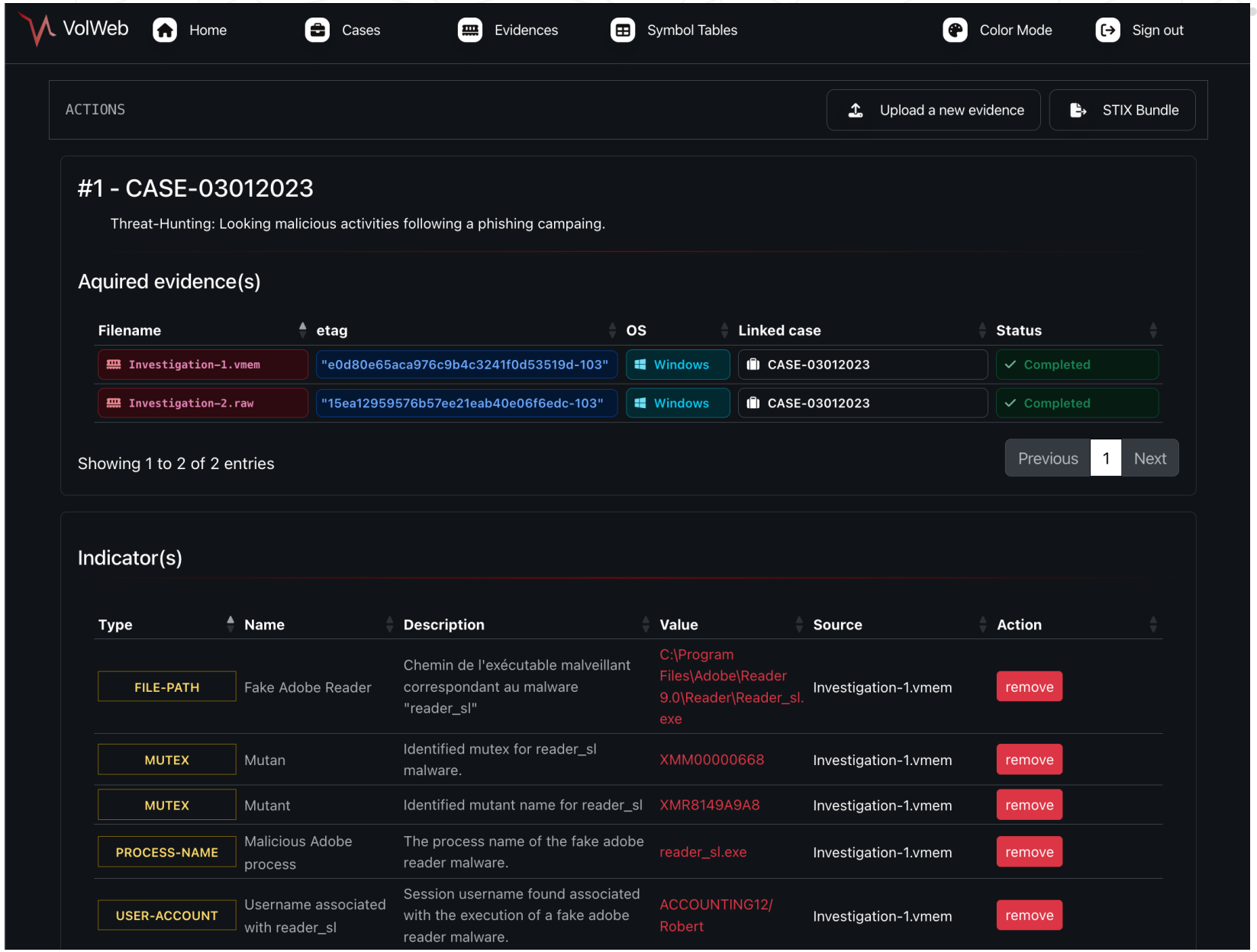
- Amélioration continue du projet (ajout de scripts, fonctionnalités, mise à jour régulières).
- Proposition de collaboration et de la potentielle migration du projet avec la volatility foundation.
- Continuer les contributions sur le framework volatility3 (support ARM, …).

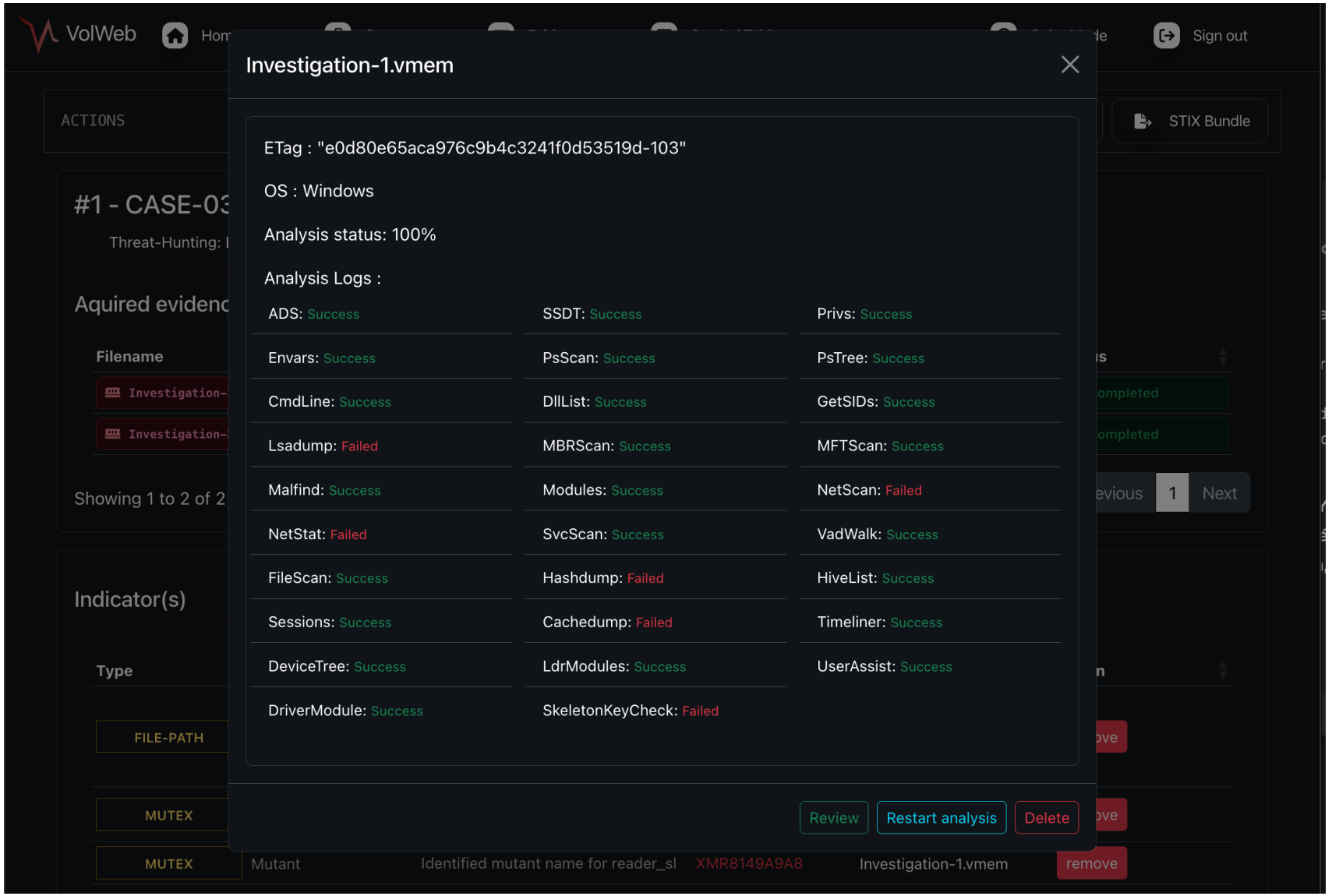
Contact:
felix.guyard@forensicxlab.com
@k1nd0ne (Twitter/Github)

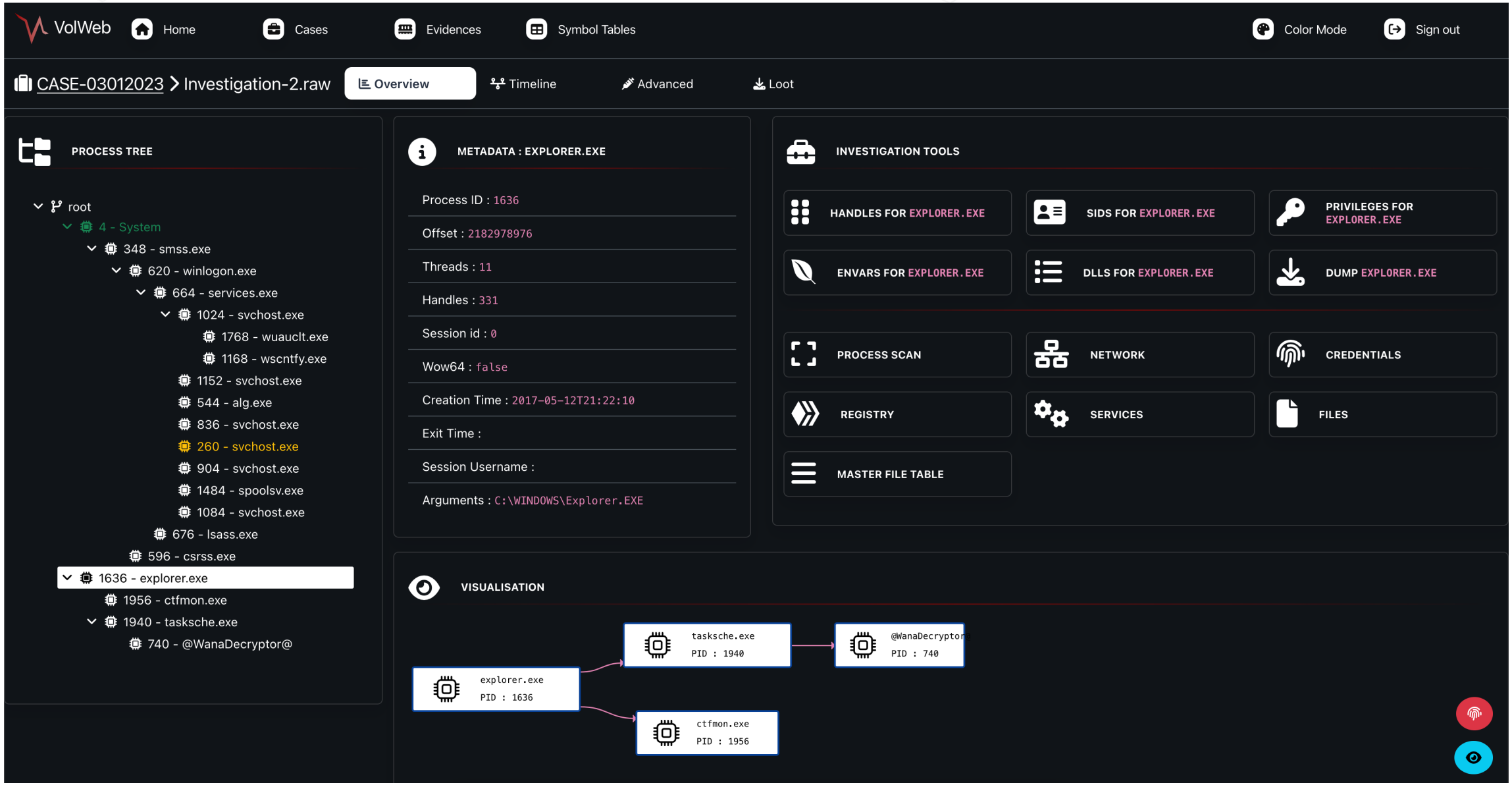
Blog : www.forensicxlab.com

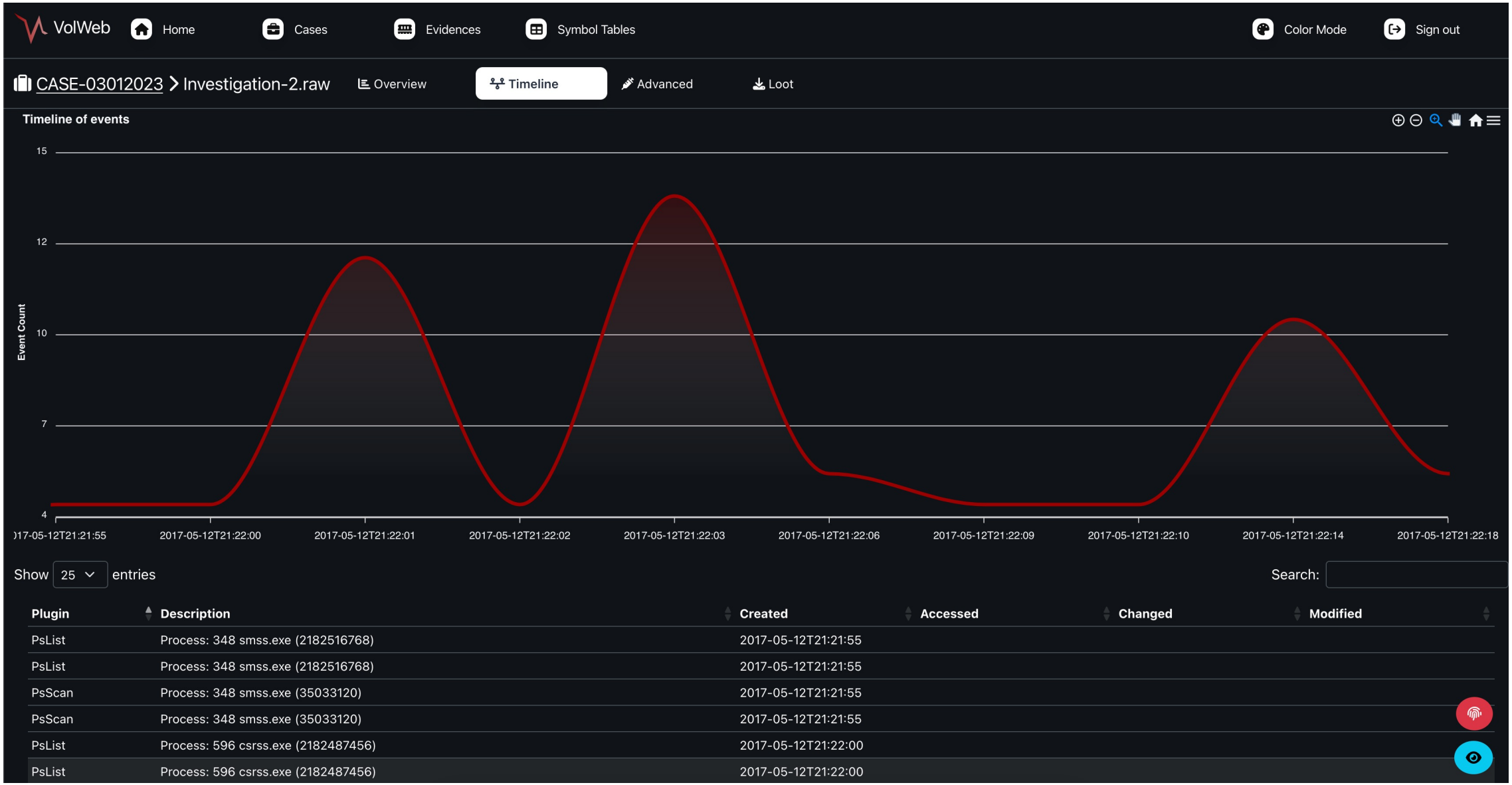

VolWeb
Home
Cases
Evidences
Symbol Tables
Color Mode
Sign out
5
EVIDENCE(S)
3
CASE(S)
11
INVESTIGATOR(S)
2
ISF
0
PROCESSING
Analysis
Started analysis in time
3.0
2.9
2.8
2.7
2.6
2.5
2.4
2.3
2.2
2.1
2.0
24-03-25
2024-03-24
Operating system repartition
Windows - 4
Linux - 1
RECENT CASES
CASE-04012024
CASE-05032024
CASE-03012023
TEAM MEMBERS
- dupont
- felix
- john
- jack
- michael
- anna
RECENT ISF
debian 5.10.0-18-amd64
debian 5.10.0-17-amd64
Copy API Token

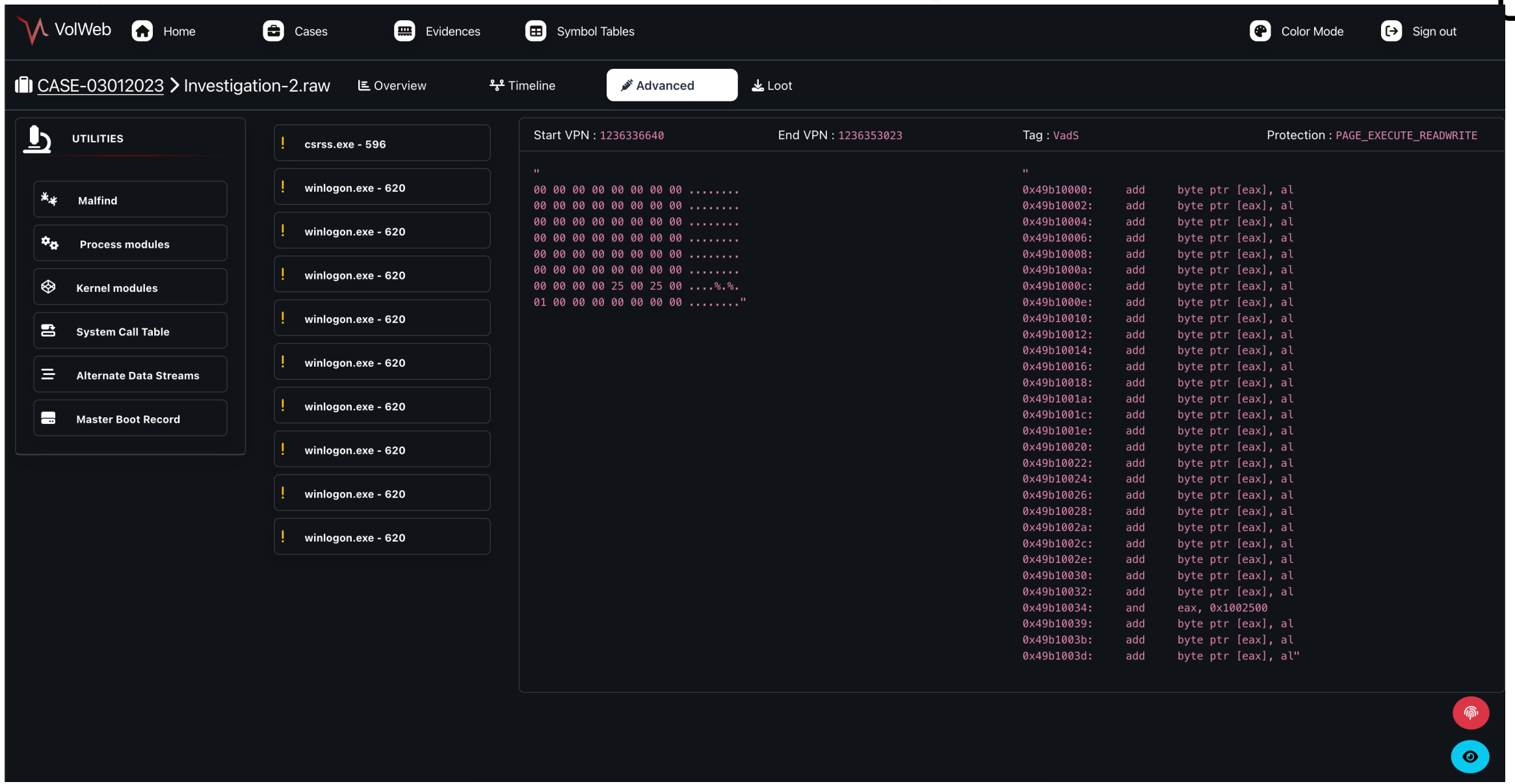

VolWeb
Home
Cases
Evidences
Symbol Tables
Color Mode
Sign out
ACTIONS
Create a case
Show 25 entries
Search:
Case No
Name
Description
Last Modified
1
CASE-03012023
Threat-Hunting: Looking malicious activities following a phishing camp...
2024-03-25
2
CASE-04012024
Réponse à incident: Compromissions suite à une campagne d'hameço...
2024-03-24
3
CASE-05032024
Threat Hunting: recherche de compromission sur les systèmes de Jean.
2024-03-25
Showing 1 to 3 of 3 entries
Case # 1: CASE-03012023
Investigators : felix, julien, vanessa
Description : Threat-Hunting: Looking malicious activities following a phishing campaing.
Evidence collection
Name
OS
Status
Investigation-1.vmem
Windows
100%
Investigation-2.raw
Windows
100%
Review
Edit
Delete
Previous
1
Next


VolWeb
Home
Cases
Evidences
Symbol Tables
Color Mode
Sign out
ACTIONS
Upload a new evidence
STIX Bundle
#1 - CASE-03012023
Threat-Hunting: Looking malicious activities following a phishing campaing.
Aquired evidence(s)
Filename
etag
OS
Linked case
Status
Investigation-1.vmem
"e0d80e65aca976c9b4c3241f0d53519d-103"
Windows
CASE-03012023
Completed
Investigation-2.raw
"15ea12959576b57ee21eab40e06f6edc-103"
Windows
CASE-03012023
Completed
Showing 1 to 2 of 2 entries
Previous
1
Next
Indicator(s)
Type
Name
Description
Value
Source
Action
FILE-PATH
Fake Adobe Reader
Chemin de l'exécutable malveillant correspondant au malware "reader_sl"
C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe
Investigation-1.vmem
remove
MUTEX
Mutan
Identified mutex for reader_sl malware.
XMM00000668
Investigation-1.vmem
remove
MUTEX
Mutant
Identified mutant name for reader_sl
XMR8149A9A8
Investigation-1.vmem
remove
PROCESS-NAME
Malicious Adobe process
The process name of the fake adobe reader malware.
reader_sl.exe
Investigation-1.vmem
remove
USER-ACCOUNT
Username associated with reader_sl
Session username found associated with the execution of a fake adobe reader malware.
ACCOUNTING12/ Robert
Investigation-1.vmem
remove

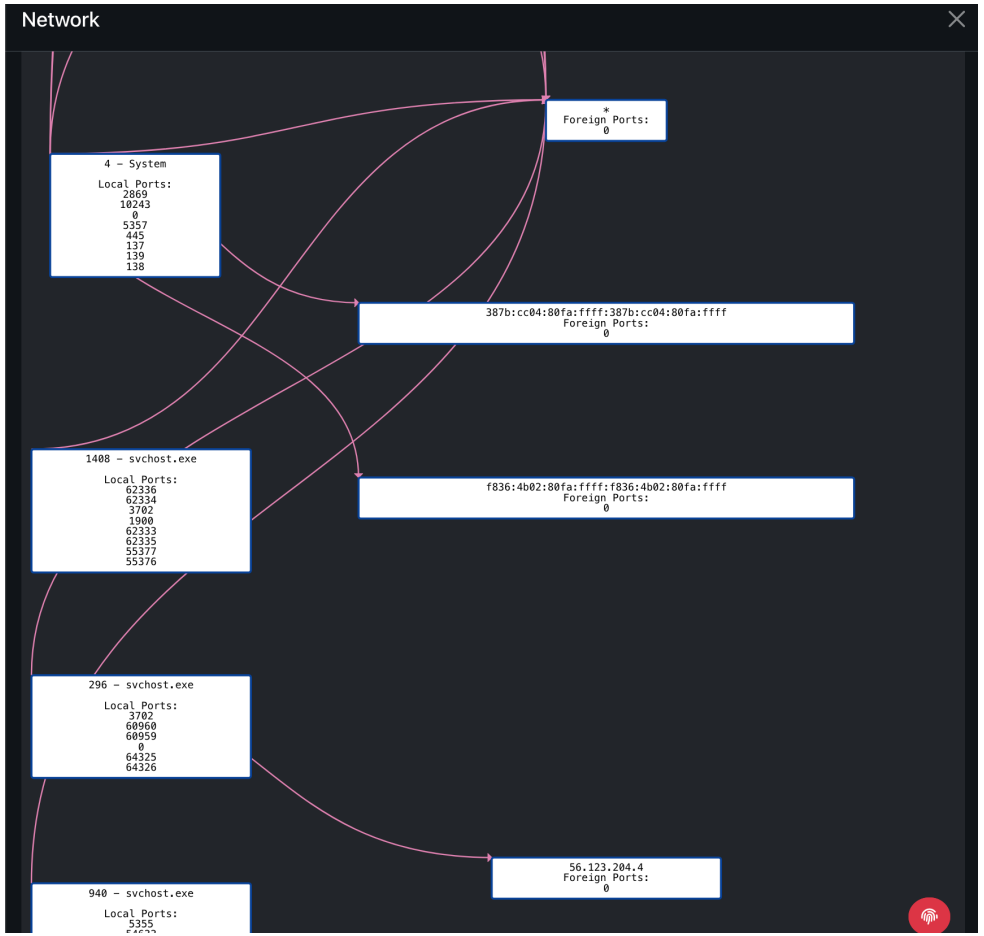

VolWeb
Sign out
ACTIONS
STIX Bundle
#1 - CASE-03
Threat-Hunting:
Aquired evidenc
Filename
Showing 1 to 2 of 2
Indicator(s)
Type
FILE-PATH
MUTEX
MUTEX
Mutant
Identified mutant name for reader_sl
XMR8149A9A8
Investigation-1.vmem
remove
Investigation-1.vmem
ETag : "e0d80e65aca976c9b4c3241f0d53519d-103"
OS : Windows
Analysis status: 100%
Analysis Logs :
ADS: Success
SSDT: Success
Privs: Success
Envars: Success
PsScan: Success
PsTree: Success
CmdLine: Success
DllList: Success
GetSIDs: Success
Lsadump: Failed
MBRScan: Success
MFTScan: Success
Malfind: Success
Modules: Success
NetScan: Failed
NetStat: Failed
SvcScan: Success
VadWalk: Success
FileScan: Success
Hashdump: Failed
HiveList: Success
Sessions: Success
Cachedump: Failed
Timeliner: Success
DeviceTree: Success
LdrModules: Success
UserAssist: Success
DriverModule: Success
SkeletonKeyCheck: Failed
Review
Restart analysis
Delete

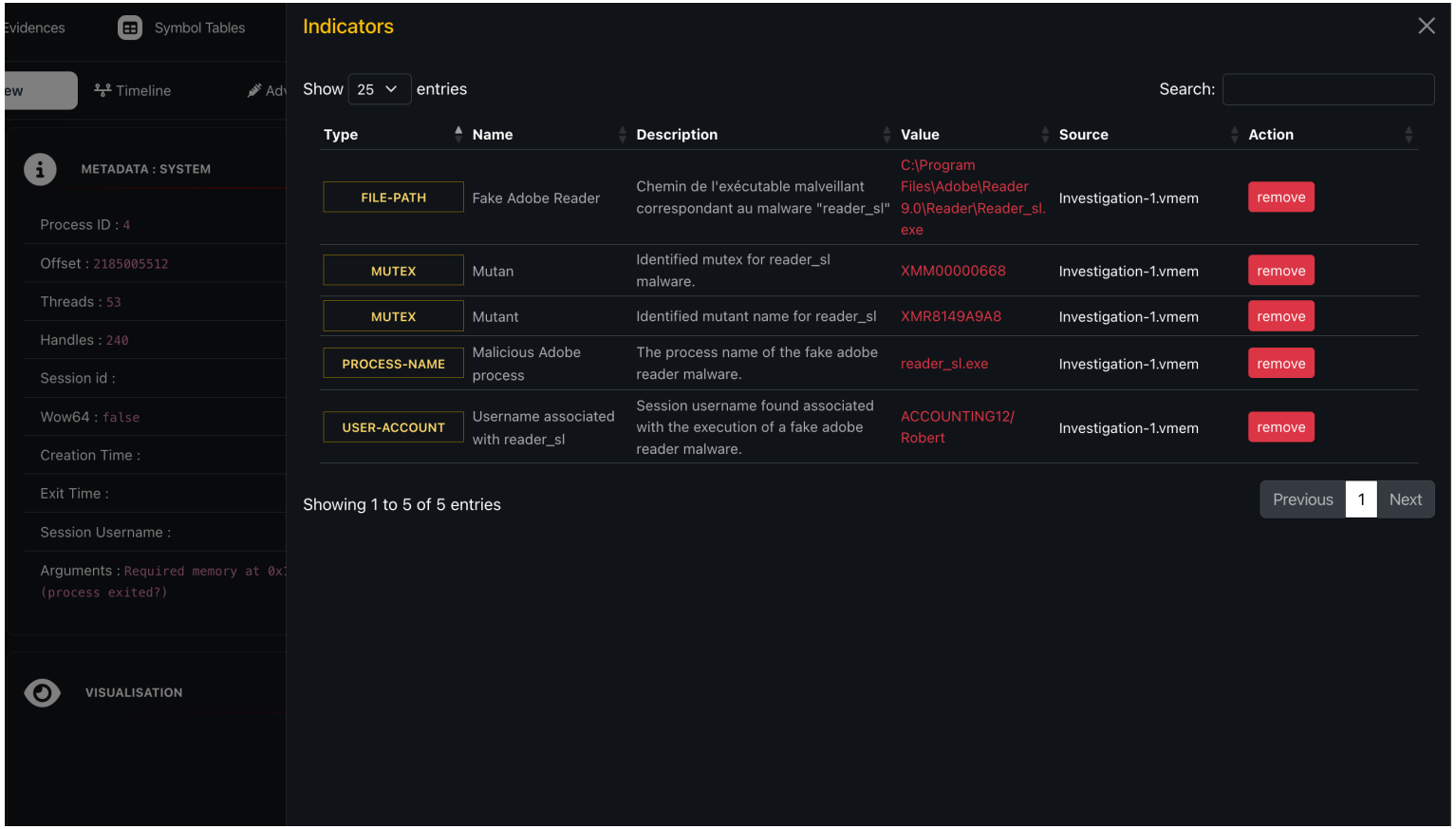

VolWeb
Home
Cases
Evidences
Symbol Tables
Color Mode
Sign out
CASE-03012023 > Investigation-2.raw
Overview
Timeline
Advanced
Loot
PROCESS TREE
root
4 - System
348 - smss.exe
620 - winlogon.exe
664 - services.exe
1024 - svchost.exe
1768 - wuauclt.exe
1168 - wscntfy.exe
1152 - svchost.exe
544 - alg.exe
836 - svchost.exe
260 - svchost.exe
904 - svchost.exe
1484 - spoolsv.exe
1084 - svchost.exe
676 - lsass.exe
596 - csrss.exe
1636 - explorer.exe
1956 - ctfmon.exe
1940 - tasksche.exe
740 - @WanaDecryptor@
METADATA : EXPLORER.EXE
Process ID : 1636
Offset : 2182978976
Threads : 11
Handles : 331
Session id : 0
Wow64 : false
Creation Time : 2017-05-12T21:22:10
Exit Time :
Session Username :
Arguments : C:\WINDOWS\Explorer.EXE
INVESTIGATION TOOLS
HANDLES FOR EXPLORER.EXE
SIDS FOR EXPLORER.EXE
PRIVILEGES FOR EXPLORER.EXE
ENVARS FOR EXPLORER.EXE
DLLS FOR EXPLORER.EXE
DUMP EXPLORER.EXE
PROCESS SCAN
NETWORK
CREDENTIALS
REGISTRY
SERVICES
FILES
MASTER FILE TABLE
VISUALISATION
tasksche.exe
PID : 1940
@WanaDecryptor
PID : 740
explorer.exe
PID : 1636
ctfmon.exe
PID : 1956


VolWeb
Home
Cases
Evidences
Symbol Tables
Color Mode
Sign out
CASE-03012023 > Investigation-2.raw
Overview
Timeline
Advanced
Loot
Timeline of events
15
12
10
7
4
Event Count
2017-05-12T21:21:55
2017-05-12T21:22:00
2017-05-12T21:22:01
2017-05-12T21:22:02
2017-05-12T21:22:03
2017-05-12T21:22:06
2017-05-12T21:22:09
2017-05-12T21:22:10
2017-05-12T21:22:14
2017-05-12T21:22:18
Show 25 entries
Search:
Plugin
Description
Created
Accessed
Changed
Modified
PsList Process: 348 smss.exe (2182516768) 2017-05-12T21:21:55
PsList Process: 348 smss.exe (2182516768) 2017-05-12T21:21:55
PsScan Process: 348 smss.exe (35033120) 2017-05-12T21:21:55
PsScan Process: 348 smss.exe (35033120) 2017-05-12T21:21:55
PsList Process: 596 csrss.exe (2182487456) 2017-05-12T21:22:00
PsList Process: 596 csrss.exe (2182487456) 2017-05-12T21:22:00


VolWeb
Home
Cases
Evidences
Symbol Tables
Color Mode
Sign out
CASE-03012023 > Investigation-2.raw
Overview
Timeline
Advanced
Loot
UTILITIES
Malfind
Process modules
Kernel modules
System Call Table
Alternate Data Streams
Master Boot Record
csrss.exe - 596
winlogon.exe - 620
winlogon.exe - 620
winlogon.exe - 620
winlogon.exe - 620
winlogon.exe - 620
winlogon.exe - 620
winlogon.exe - 620
winlogon.exe - 620
Start VPN : 1236336640
End VPN : 1236353023
Tag : VadS
Protection : PAGE_EXECUTE_READWRITE
00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 ....
00 00 00 00 25 00 25 00 ....%.%.
01 00 00 00 00 00 00 00 ....
0x49b10000: add byte ptr [eax], al
0x49b10002: add byte ptr [eax], al
0x49b10004: add byte ptr [eax], al
0x49b10006: add byte ptr [eax], al
0x49b10008: add byte ptr [eax], al
0x49b1000a: add byte ptr [eax], al
0x49b1000c: add byte ptr [eax], al
0x49b1000e: add byte ptr [eax], al
0x49b10010: add byte ptr [eax], al
0x49b10012: add byte ptr [eax], al
0x49b10014: add byte ptr [eax], al
0x49b10016: add byte ptr [eax], al
0x49b10018: add byte ptr [eax], al
0x49b1001a: add byte ptr [eax], al
0x49b1001c: add byte ptr [eax], al
0x49b1001e: add byte ptr [eax], al
0x49b10020: add byte ptr [eax], al
0x49b10022: add byte ptr [eax], al
0x49b10024: add byte ptr [eax], al
0x49b10026: add byte ptr [eax], al
0x49b10028: add byte ptr [eax], al
0x49b1002a: add byte ptr [eax], al
0x49b1002c: add byte ptr [eax], al
0x49b1002e: add byte ptr [eax], al
0x49b10030: add byte ptr [eax], al
0x49b10032: add byte ptr [eax], al
0x49b10034: and eax, 0x1002500
0x49b10039: add byte ptr [eax], al
0x49b1003b: add byte ptr [eax], al
0x49b1003d: add byte ptr [eax], al

5 –


Network
*
Foreign Ports:
0
4 – System
Local Ports:
2869
10243
0
5357
445
137
139
138
387b:cc04:80fa:ffff:387b:cc04:80fa:ffff
Foreign Ports:
0
1408 – svchost.exe
Local Ports:
62336
62334
3702
1900
62333
62335
55377
55376
f836:4b02:80fa:ffff:f836:4b02:80fa:ffff
Foreign Ports:
0
296 – svchost.exe
Local Ports:
3702
60960
60959
0
64325
64326
56.123.204.4
Foreign Ports:
0
940 – svchost.exe
Local Ports:
5355


Evidences
Symbol Tables
Timeline
METADATA : SYSTEM
Process ID : 4
Offset : 2185005512
Threads : 53
Handles : 240
Session id :
Wow64 : false
Creation Time :
Exit Time :
Session Username :
Arguments : Required memory at 0x
(process exited?)
VISUALISATION
Indicators
Show 25 entries
Search:
Type
Name
Description
Value
Source
Action
FILE-PATH
Fake Adobe Reader
Chemin de l'exécutable malveillant correspondant au malware "reader_sl"
C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe
Investigation-1.vmem
remove
MUTEX
Mutan
Identified mutex for reader_sl malware.
XMM00000668
Investigation-1.vmem
remove
MUTEX
Mutant
Identified mutant name for reader_sl
XMR8149A9A8
Investigation-1.vmem
remove
PROCESS-NAME
Malicious Adobe process
The process name of the fake adobe reader malware.
reader_sl.exe
Investigation-1.vmem
remove
USER-ACCOUNT
Username associated with reader_sl
Session username found associated with the execution of a fake adobe reader malware.
ACCOUNTING12/ Robert
Investigation-1.vmem
remove
Showing 1 to 5 of 5 entries
Previous
1
Next