



SECURITY IS

COMPTE RENDU PROJET STATIC ANALYSIS

Équipe

BIAOU Afouda Jean Paul
SIMPORE Idriss
YA Roxane

Enseignant

Max AGUEH

Analyse de vulnérabilités logiciels (Analyse Statique)

EXERCICE 1

1- Importation du LAB virtuel AVL-LAB.ova sur Virtualbox :

Effectuer

2- Configuration de l'interface réseau :

sudo ifup enp0s3

3- Décompression avec unzip :

Effectuer

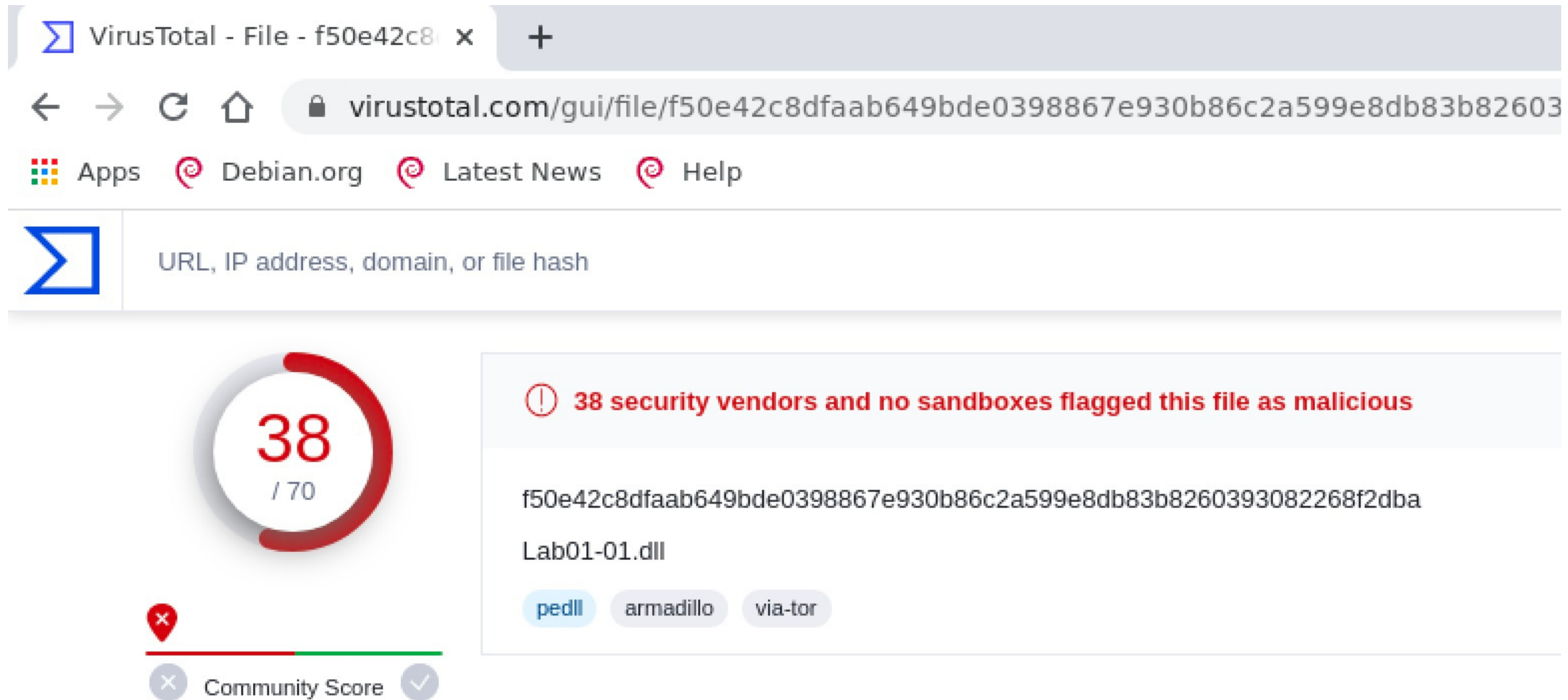
4- Mettez à jour la VM :

fast-update install_avl

5- Chargez les fichiers ii.exe et tp1\lab0101.dll dans www.VirusTotal.com.

Effectuer

6-



The screenshot shows the VirusTotal web interface. The browser tab is titled "VirusTotal - File - f50e42c8". The address bar shows the URL: `virustotal.com/gui/file/f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba`. Below the address bar, there are links for "Apps", "Debian.org", "Latest News", and "Help". The main content area features a large circular progress indicator showing a score of 38 out of 70. To the right of the progress indicator, a red warning icon is followed by the text: "38 security vendors and no sandboxes flagged this file as malicious". Below this, the file hash `f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba` and the filename "Lab01-01.dll" are displayed. At the bottom, there are three buttons: "pedll", "armadillo", and "via-tor". A "Community Score" section is visible at the bottom left, showing a red location pin icon and a progress bar.

VirusTotal - File - f50e42c8 x +

← → ↻ 🏠 [virustotal.com/gui/file/f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba](#)

📱 Apps 🌐 Debian.org 🌐 Latest News 🌐 Help

📁 URL, IP address, domain, or file hash

38 / 70

⚠️ 38 security vendors and no sandboxes flagged this file as malicious

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

Lab01-01.dll

pedll armadillo via-tor

📍 Community Score

Oui, ce fichier correspond à une signature d'antivirus de malwares connus.

7-

```
[0x100012fa]> iI | grep --color=auto compiled
compiled Sun Dec 19 17:16:38 2010
[0x100012fa]> 
```

◀ Bureau 1 ▶ 01 juil., sam. 23:23:18 ◀ ▶

- Les fichiers on été compiler pour la dernier fois le 19 Décembre 2010 à 17 H 16.

On peut conclure que les fichiers sont anciens et ont été compilés il y a un certain temps. Cela pourrait indiquer qu'ils ne sont pas récemment mis à jour et pourraient présenter des vulnérabilités de sécurité connues.

- Les APIs utilisées

compiled Sun Dec 19 17:16:38 2010

[0x100012fa]> ii

[Imports]

nth	vaddr	bind	type	lib	name
1	0x10002000	NONE	FUNC	KERNEL32.dll	Sleep
2	0x10002004	NONE	FUNC	KERNEL32.dll	CreateProcessA
3	0x10002008	NONE	FUNC	KERNEL32.dll	CreateMutexA
4	0x1000200c	NONE	FUNC	KERNEL32.dll	OpenMutexA
5	0x10002010	NONE	FUNC	KERNEL32.dll	CloseHandle
23	0x10002030	NONE	FUNC	WS2_32.dll	socket
115	0x10002034	NONE	FUNC	WS2_32.dll	WSAStartup
11	0x10002038	NONE	FUNC	WS2_32.dll	inet_addr
4	0x1000203c	NONE	FUNC	WS2_32.dll	connect
19	0x10002040	NONE	FUNC	WS2_32.dll	send
22	0x10002044	NONE	FUNC	WS2_32.dll	shutdown
16	0x10002048	NONE	FUNC	WS2_32.dll	recv
3	0x1000204c	NONE	FUNC	WS2_32.dll	closesocket
116	0x10002050	NONE	FUNC	WS2_32.dll	WSACleanup
9	0x10002054	NONE	FUNC	WS2_32.dll	htons
1	0x10002018	NONE	FUNC	MSVCRT.dll	_adjust_fdiv
2	0x1000201c	NONE	FUNC	MSVCRT.dll	malloc
3	0x10002020	NONE	FUNC	MSVCRT.dll	_initterm
4	0x10002024	NONE	FUNC	MSVCRT.dll	free
5	0x10002028	NONE	FUNC	MSVCRT.dll	strncmp

- La taille de chaque section sur disque et en mémoire, les noms des sections, leur nombre et leur contenu

```
[0x100012fa]> iS
[Sections]

nth  paddr          size  vaddr          vsize  perm  type  name
-----
0    0x00001000    0x1000 0x10001000    0x1000 -r-x  ---  .text
1    0x00002000    0x24000 0x10002000    0x24000 -r-  ---  .rdata
2    0x000026000    0x1000 0x100026000    0x1000 -rw-  ---  .data
3    0x000027000    0x1000 0x100027000    0x1000 -r-  ---  .reloc
```

- Le fichier est-il compressé "packed" ?

Non, le fichier n'est pas packé.

Un fichier "packed" est un fichier qui a été compressé ou chiffré afin de masquer son contenu réel. En effet, un fichier packé est un fichier exécutable qui a été compressé à l'aide d'un outil spécifique appelé "packer". L'objectif principal du packing est de réduire la taille du fichier exécutable, ce qui peut faciliter le transfert du fichier sur un réseau ou son stockage sur un support de stockage limité.

```

103040
[0x100012fa]> iz
[Strings]
nth  paddr      vaddr      len  size  section  type  string
-----
0     0x0000210a  0x1000210a  11   12    .rdata   ascii  CloseHandle
1     0x00002118  0x10002118   5    6    .rdata   ascii  Sleep
2     0x00002120  0x10002120  14   15    .rdata   ascii  CreateProcessA
3     0x00002132  0x10002132  12   13    .rdata   ascii  CreateMutexA
4     0x00002142  0x10002142  10   11    .rdata   ascii  OpenMutexA
5     0x0000214e  0x1000214e  12   13    .rdata   ascii  KERNEL32.dll
6     0x0000215c  0x1000215c  10   11    .rdata   ascii  WS2_32.dll
7     0x0000216a  0x1000216a   7    8    .rdata   ascii  strncmp
8     0x00002172  0x10002172  10   11    .rdata   ascii  MSVCRT.dll
9     0x00002180  0x10002180   4    5    .rdata   ascii  free
10    0x00002188  0x10002188   9   10    .rdata   ascii  _initterm
11    0x00002194  0x10002194   6    7    .rdata   ascii  malloc
12    0x0000219e  0x1000219e  12   13    .rdata   ascii  _adjust_fdiv
0     0x00026010  0x10026010   4    5    .data    ascii  exec
1     0x00026018  0x10026018   5    6    .data    ascii  sleep
2     0x00026020  0x10026020   5    6    .data    ascii  hello
3     0x00026028  0x10026028  13   14    .data    ascii  127.26.152.13
4     0x00026038  0x10026038   8    9    .data    ascii  SADFHUHF
[0x100012fa]> 

```

8- Que pouvez-vous dire sur le comportement du fichier en analysant les fonctions importées et les chaînes de caractères retrouvés.

D'après l'analyse des fonctions importées et des chaînes de caractères retrouvées, il est possible de conclure que le fichier semble être un programme Windows. Les chaînes de caractères identifiées font référence à des fonctions, bibliothèques et messages spécifiques à l'environnement Windows. Cela suggère que le fichier est conçu pour s'exécuter sur un système d'exploitation Windows et interagir avec les API Windows pour effectuer certaines actions.

EXERCICE 2

1- Chargez les fichiers ~/malware_samples/fichiers_cours_malwares/tp1/lab01- 02.exe dans www.VirusTotal.com


Oui, ce fichier correspond à une signature d'antivirus de malwares connus.

VirusTotal - File - f50e42c8 x | VirusTotal - File - 58898bd4 x | VirusTotal - File - c876a332 x +

← → ↻ 🏠 virustotal.com/gui/file/c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

📱 Apps 🌐 Debian.org 🌐 Latest News 🌐 Help

🔍 c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6



55
/ 70

📍
Community Score

⚠️ 55 security vendors and 1 sandbox flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Lab01-02.exe

peexe checks-disk-space via-tor detect-debug-environment idle long-sleeps upx checks-user-input

2- Refaites les mêmes étapes que lors de l'exercice 1

```

debian@debian:~/malware_samples/fichiers_cours_malwares$ radare
2 -A tp1/Lab01-02.exe
INFO: Analyze all flags starting with sym. and entry0 (aa)
INFO: Analyze all functions arguments/locals (afva@@@F)
INFO: Analyze function calls (aac)
INFO: Analyze len bytes of instructions for references (aar)
INFO: Finding and parsing C++ vtables (avrr)
INFO: Type matching analysis for all functions (aافت)
INFO: Propagate noreturn information (aanr)
INFO: Use -AA or aaaa to perform additional experimental analysis
is
-- Seek at relative offsets with 's +<offset>' or 's -<offset>'

```

- Quelle est la date/heure de compilation.

Il a été compilé pour la dernière fois le Mercredi 19 janvier 2011 à 17h10

```

-- Seek at relative offsets with 's +<offset>' or 's -<offset>'
[0x00405410]> iI | grep --color=auto compiled
compiled Wed Jan 19 17:10:41 2011
[0x00405410]> ii
[Imports]
nth vaddr      bind type lib      name

```


D'après la date et l'heure de compilation du fichier, qui remonte au mercredi 19 janvier 2011 à 17h10, on peut en tirer la conclusion que le fichier a été créé il y a un certain temps. Cela suggère que le fichier est ancien et n'a pas été modifié depuis cette date.

- les APIs utilisées

```
[0x00405410]> ii
[Imports]
nth vaddr      bind type lib      name
-----
1  0x00406064  NONE FUNC  KERNEL32.DLL  LoadLibraryA
2  0x00406068  NONE FUNC  KERNEL32.DLL  GetProcAddress
3  0x0040606c  NONE FUNC  KERNEL32.DLL  VirtualProtect
4  0x00406070  NONE FUNC  KERNEL32.DLL  VirtualAlloc
5  0x00406074  NONE FUNC  KERNEL32.DLL  VirtualFree
6  0x00406078  NONE FUNC  KERNEL32.DLL  ExitProcess
1  0x00406080  NONE FUNC  ADVAPI32.dll  CreateServiceA
1  0x00406088  NONE FUNC  MSVCRT.dll    exit
1  0x00406090  NONE FUNC  WININET.dll   InternetOpenA
```


- La taille de chaque section sur disque et en mémoire, les noms des sections, leur nombre et leur contenu

```
[0x00405410]> iS
[Sections]

nth  paddr          size  vaddr          vsize perm  type  name
-----
0    0x000000400     0x0  0x00401000     0x4000 -rwx  - - - - UPX0
1    0x000000400     0x600 0x00405000     0x1000 -rwx  - - - - UPX1
2    0x000000a00     0x200 0x00406000     0x1000 -rw-  - - - - UPX2
```

- Le fichier est-il compressé "packed" ?

Oui, le fichier est packé.

```
[0x00405410]> iz
[Strings]
nth  paddr  vaddr  len  size  section  type  string
-----
```

Nous avons conclu précédemment que le fichier était packé, nous allons le décompresser et refaire les analyses

- Fichier décompresser

```
debian@debian:~/malware_samples/fichiers_cours_malwares$ upx -d
tp1/Lab01-02.exe -o tp1/unpacked.exe
                Ultimate Packer for eXecutables
                Copyright (C) 1996 - 2018
UPX 3.95          Markus Oberhumer, Laszlo Molnar & John Reiser
Aug 26th 2018

      File size      Ratio      Format      Name
-----
    16384 <-    3072    18.75%    win32/pe    unpacked.exe

Unpacked 1 file.
```

```

debian@debian:~/malware_samples/fichiers_cours_malwares$ radare
2 -A tpl/unpacked.exe
INFO: Analyze all flags starting with sym. and entry0 (aa)
INFO: Analyze all functions arguments/locals (afva@@@F)
INFO: Analyze function calls (aac)
INFO: Analyze len bytes of instructions for references (aar)
INFO: Finding and parsing C++ vtables (avrr)
INFO: Type matching analysis for all functions (aافت)
INFO: Propagate noreturn information (aanr)
INFO: Use -AA or aaaa to perform additional experimental analysis
is
-- For a full documentation see `r2 -qc iz /lib/libr_core.so`

```

- La date/heure de compilation de chaque fichier

```

[0x00401190]> iI | grep --color=auto compiled
compiled Wed Jan 19 17:10:41 2011

```

- Les APIs utilisées


```
[0x00401190]> ii
```

```
[Imports]
```

nth	vaddr	bind	type	lib	name
1	0x00402010	NONE	FUNC	KERNEL32.DLL	SystemTimeToFileTime
2	0x00402014	NONE	FUNC	KERNEL32.DLL	GetModuleFileNameA
3	0x00402018	NONE	FUNC	KERNEL32.DLL	CreateWaitableTimerA
4	0x0040201c	NONE	FUNC	KERNEL32.DLL	ExitProcess
5	0x00402020	NONE	FUNC	KERNEL32.DLL	OpenMutexA
6	0x00402024	NONE	FUNC	KERNEL32.DLL	SetWaitableTimer
7	0x00402028	NONE	FUNC	KERNEL32.DLL	WaitForSingleObject
8	0x0040202c	NONE	FUNC	KERNEL32.DLL	CreateMutexA
9	0x00402030	NONE	FUNC	KERNEL32.DLL	CreateThread
1	0x00402000	NONE	FUNC	ADVAPI32.dll	CreateServiceA
2	0x00402004	NONE	FUNC	ADVAPI32.dll	StartServiceCtrlDispatcherA
3	0x00402008	NONE	FUNC	ADVAPI32.dll	OpenSCManagerA
1	0x00402038	NONE	FUNC	MSVCRT.dll	_exit
2	0x0040203c	NONE	FUNC	MSVCRT.dll	_XcptFilter
3	0x00402040	NONE	FUNC	MSVCRT.dll	exit
4	0x00402044	NONE	FUNC	MSVCRT.dll	__p__initenv
5	0x00402048	NONE	FUNC	MSVCRT.dll	__getmainargs
6	0x0040204c	NONE	FUNC	MSVCRT.dll	_initterm
7	0x00402050	NONE	FUNC	MSVCRT.dll	__setusermatherr
8	0x00402054	NONE	FUNC	MSVCRT.dll	_adjust_fdiv
9	0x00402058	NONE	FUNC	MSVCRT.dll	__p__commode
10	0x0040205c	NONE	FUNC	MSVCRT.dll	__p__fmode
11	0x00402060	NONE	FUNC	MSVCRT.dll	__set_app_type
12	0x00402064	NONE	FUNC	MSVCRT.dll	_except_handler3
13	0x00402068	NONE	FUNC	MSVCRT.dll	_controlfp
1	0x00402070	NONE	FUNC	WININET.dll	InternetOpenUrlA
2	0x00402074	NONE	FUNC	WININET.dll	InternetOpenA

- La taille de chaque section sur disque et en mémoire, les noms des sections, leur nombre et leur contenu

```
[0x00401190]> iS
[Sections]

nth  paddr          size  vaddr          vsize  perm  type  name
-----
0    0x00001000    0x1000 0x00401000    0x1000 -r-x  ---  .text
1    0x00002000    0x1000 0x00402000    0x1000 -r-   ---  .rdata
2    0x00003000    0x1000 0x00403000    0x1000 -rw-  ---  .data
```

- Le fichier n'est plus packed


```

[0x00401190]> iz
[Strings]
nth paddr      vaddr      len size section type  string
-----
0  0x0000216c 0x0040216c 12  13  .rdata  ascii  KERNEL32.DLL
1  0x00002179 0x00402179 12  13  .rdata  ascii  ADVAPI32.dll
2  0x00002186 0x00402186 10  11  .rdata  ascii  MSVCRT.dll
3  0x00002191 0x00402191 11  12  .rdata  ascii  WININET.dll
4  0x000021a0 0x004021a0 20  21  .rdata  ascii  SystemTimeToF
leTime
5  0x000021b6 0x004021b6 18  19  .rdata  ascii  GetModuleFile
ameA
6  0x000021ca 0x004021ca 20  21  .rdata  ascii  CreateWaitabl
TimerA
7  0x000021e0 0x004021e0 11  12  .rdata  ascii  ExitProcess
8  0x000021ee 0x004021ee 10  11  .rdata  ascii  OpenMutexA
9  0x000021fa 0x004021fa 16  17  .rdata  ascii  SetWaitableTi
er
10 0x0000220c 0x0040220c 19  20  .rdata  ascii  WaitForSingle
bject
11 0x00002222 0x00402222 12  13  .rdata  ascii  CreateMutexA
12 0x00002230 0x00402230 12  13  .rdata  ascii  CreateThread
13 0x0000223e 0x0040223e 14  15  .rdata  ascii  CreateService
14 0x0000224e 0x0040224e 27  28  .rdata  ascii  StartServiceC
rlDispatcherA
15 0x0000226c 0x0040226c 14  15  .rdata  ascii  OpenSCManager
16 0x0000227c 0x0040227c 5   6   .rdata  ascii  _exit
17 0x00002284 0x00402284 11  12  .rdata  ascii  _XcptFilter
18 0x00002292 0x00402292 4   5   .rdata  ascii  exit
19 0x00002298 0x00402298 13  14  .rdata  ascii  __p___initenv
20 0x000022a8 0x004022a8 13  14  .rdata  ascii  __getmainargs
21 0x000022b8 0x004022b8 9   10  .rdata  ascii  _initterm
22 0x000022c4 0x004022c4 16  17  .rdata  ascii  __setusermath
rr
23 0x000022d6 0x004022d6 12  13  .rdata  ascii  _adjust_fdiv
24 0x000022e4 0x004022e4 12  13  .rdata  ascii  __p__commode
25 0x000022f2 0x004022f2 10  11  .rdata  ascii  __p__fmode

```


Ce Que pouvez-vous dire : Ces informations indiquent que le fichier peut être un programme exécutable Windows standard qui interagit avec le système d'exploitation en utilisant les fonctions importées. Il peut effectuer des opérations telles que la gestion des threads, la création de services, l'administration des processus et l'utilisation des fonctions de la bibliothèque C Runtime.

MERCI !