



SEC 102 - TP05

Étude du format PE

Date	Version	Description	Auteurs
19/03/2023	1	Retranscription collective des informations présentées en cours	Bartel Cantin Bialas Alexis Dufourt Marvin Faussurier Marc N'Guessan Jérémy

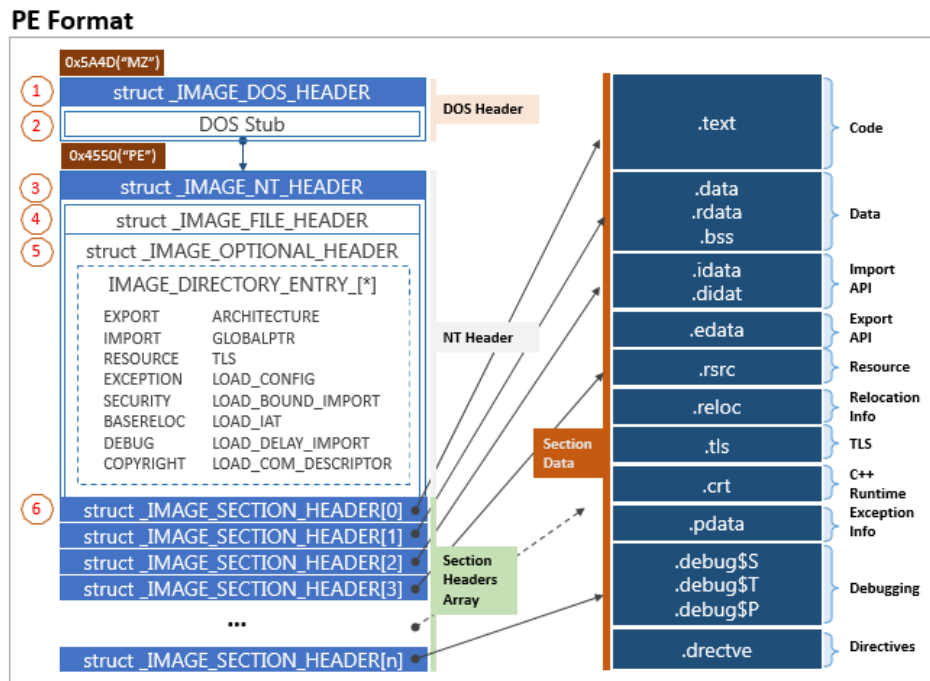
Sommaire :

1. Résumé explicatif et visuel du format PE	2
2. Quelles sont les extensions de fichiers qui ont un format PE?	4
3. Quelle signature HEXA le format PE prend-il ?	5
4. Sous quels SE retrouve-t-on le format PE ?	6
5. Que se passe-t-il si Windows ne reconnaît pas le format PE pour le fichier ?	7
6. Dans quelle partie de la structure PE, trouve-t-on le TimeDateStamp ?	8
7. Combien peut-il y avoir de Sections dans le format PE?	9
8. Dans quelle partie de la Section trouve-t-on le code du programme ?	10
9. Qu'est-ce qu'un packer et à quoi peut-il servir ?	11
10. Quels logiciels peuvent vous aider à analyser un fichier au format PE ?	12
12. Glossaire	14

1. Résumé explicatif et visuel du format PE

Le format PE (Portable Executable) est un format de fichier binaire utilisé principalement pour les fichiers exécutables Windows, tels que les applications, les bibliothèques de liens dynamiques (DLL) et les pilotes.

Le but principal de ce format est de fournir un moyen standard pour stocker les informations nécessaires à l'exécution d'un programme sur une machine Windows.



Le format PE fournit des informations sur :

- la taille de l'image exécutable
- son adresse de base
- les sections et les entêtes
- les tables d'importation et d'exportation
- les ressources et les symboles
- ainsi que d'autres informations nécessaires à l'exécution du programme.

Le format PE permet d'ajouter des ressources personnalisées à un programmes tels que :

- des icônes
- des images
- des sons

Il permet également de lier dynamiquement des bibliothèques externes à un programme, ce qui peut réduire la taille de l'exécutable et faciliter la maintenance.

En résumé, le format PE est un format de fichier standard utilisé pour stocker les informations nécessaires à l'exécution d'un programme sur une machine Windows. Il fournit des informations critiques sur l'image exécutable et offre une flexibilité et une extensibilité considérables.

Fichier		Maj																Maj	
bonjour.exe		Maj																Maj	
Maj		Maj																Maj	
Offset (h)		00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé	
00000810	7C 2A 88 03 C6 49 88 03 4D 70 43 6F 6E 66 69 67																	*^..EI^..MpConfig	
00000820	43 6C 6F 73 65 00 00 00 4D 70 43 6F 6E 66 69 67																	Close...MpConfig	
00000830	47 65 74 56 61 6C 75 65 00 00 00 00 4D 70 43 6F																	GetValue....MpCo	
00000840	6E 66 69 67 4F 70 65 6E 00 00 00 00 4D 70 54 68																	nfigOpen....MpTh	
00000850	72 65 61 74 45 6E 75 6D 65 72 61 74 65 00 00 00																	reatEnumerate...	
00000860	4D 70 54 68 72 65 61 74 4F 70 65 6E 00 00 00 00																	MpThreatOpen....	
00000870	4D 70 53 63 61 6E 52 65 73 75 6C 74 00 00 00 00																	MpScanResult....	
00000880	4D 70 53 63 61 6E 53 74 61 72 74 00 4D 70 46 72																	MpScanStart..MpFr	
00000890	65 65 4D 65 6D 6F 72 79 00 00 00 00 4D 70 48 61																	eeMemory....MpHa	
000008A0	6E 64 6C 65 43 6C 6F 73 65 00 00 00 4D 70 4D 61																	ndleClose...MpMa	
000008B0	6E 61 67 65 72 4F 70 65 6E 00 00 00 25 00 73 00																	nagerOpen...%.s.	

2. Quelles sont les extensions de fichiers qui ont un format PE?

Les extensions utilisées sont les suivantes : .cpl, .exe, .dll, .ocx, .sys, .scr, .drv, .efi .

3. Quelle signature HEXA le format PE prend-il ?

Le format PE (Portable Executable) utilise la signature HEXA "4D 5A" comme signature de début de fichier. Cette signature correspond aux lettres "MZ" en ASCII, qui font référence à Mark Zbikowski, un développeur de Microsoft qui a participé au développement du format de fichier.

FD AD		bonjour.exe		FD AD		MpOAV.dll											
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	F0	00	00	00&....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°...'.í!..Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode.....\$.....
00000080	CE	16	73	C7	8A	77	1D	94	8A	77	1D	94	8A	77	1D	94	í.sçŠw."Šw."Šw."
00000090	83	0F	88	94	82	77	1D	94	83	0F	9E	94	98	77	1D	94	f.^",w."f.Ž"~w."
000000A0	8A	77	1C	94	3E	77	1D	94	83	0F	8E	94	87	77	1D	94	Šw.">w."f.Ž"~w."
000000B0	83	0F	8F	94	8B	77	1D	94	83	0F	99	94	A1	77	1D	94	f.."<w."f.™";w."
000000C0	83	0F	89	94	8B	77	1D	94	83	0F	8C	94	8B	77	1D	94	f.%"<w."f.€"<w."
000000D0	52	69	63	68	8A	77	1D	94	00	00	00	00	00	00	00	00	RichŠw.".....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

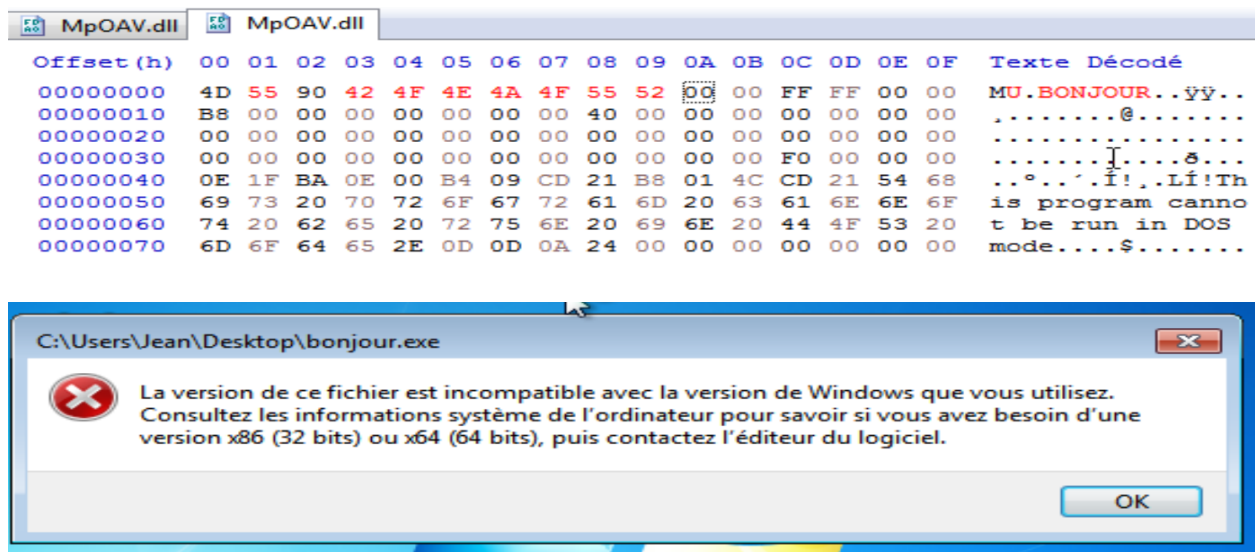
4. Sous quels SE retrouve-t-on le format PE ?

Le format PE est utilisé sous Windows, de sa première version Windows NT 3.1 sortie en 1993 à sa dernière version Windows 11.

5. Que se passe-t-il si Windows ne reconnaît pas le format PE pour le fichier ?

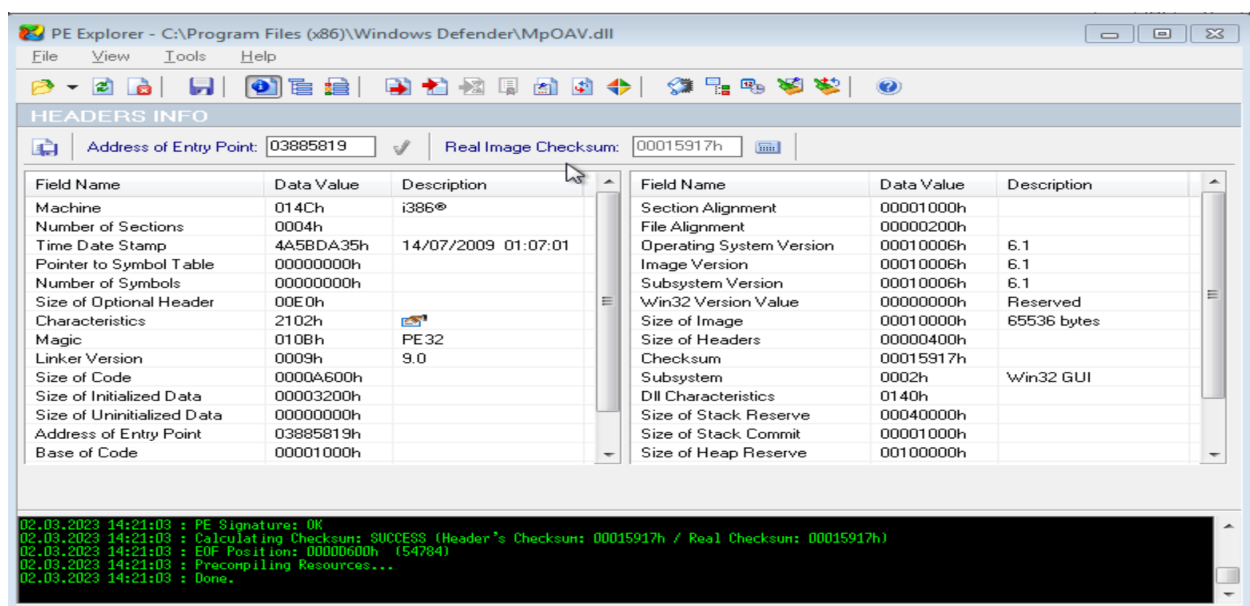
Si Windows ne reconnaît pas le format PE d'un fichier alors celui-ci devient inutilisable.

Un fichier qui n'est pas au format PE est soit corrompu, soit destiné à une autre plateforme.



6. Dans quelle partie de la structure PE, trouve-t-on le TimeDateStamp ?

Cela correspond à la **date de compilation ou de liaison** de l'exécutable. C'est utile pour des tâches de maintenance mais c'est une donnée très facilement modifiable et donc peu fiable dans le cadre d'une analyse statique de malware.



7. Combien peut-il y avoir de Sections dans le format PE?

Le nombre de sections dans un fichier PE peut varier en fonction du compilateur utilisé pour générer le fichier et des options de compilation spécifiées.

En général, un fichier PE peut avoir de 1 à plusieurs dizaines de sections.

Les sections couramment trouvées dans un fichier PE sont :

- `.text` : contient le code exécutable
- `.rdata` : contient des données en lecture seule (constantes, messages d'erreur, etc.)
- `.data` : contient des données initialisées (variables globales, etc.)
- `.rsrc` : contient des ressources (icônes, images, etc.)

D'autres sections telles que `.idata`, `.reloc`, `.debug`, `.tls` peuvent également être présentes en fonction des besoins de l'application.

8. Dans quelle partie de la Section trouve-t-on le code du programme ?

Le code exécutable d'un programme se trouve généralement dans la section `.text`.

La section `.text` est une section obligatoire dans un fichier PE et contient le code binaire compilé à partir du code source du programme.

Cette section est généralement marquée comme exécutable et peut également être marquée comme en lecture seule pour protéger le code contre toute modification accidentelle.

9. Qu'est-ce qu'un packer et à quoi peut-il servir ?

Un packer est un petit programme dont le but est de compresser un logiciel afin de réduire sa taille initiale, tout en conservant son aspect exécutable.

10. Quels logiciels peuvent vous aider à analyser un fichier au format PE ?

- **IDA Pro** : c'est un outil populaire pour l'analyse de code binaire. Il permet de désassembler, de décompiler et d'analyser le code exécutable pour comprendre son fonctionnement.
- **PE Explorer** : c'est un outil de visualisation et d'édition de fichiers PE. Il permet d'explorer la structure du fichier, de visualiser les ressources, d'éditer les en-têtes et les sections, et de modifier les propriétés des fichiers.
- **Ghidra** : c'est un outil open-source d'analyse de code binaire développé par la NSA. Il permet de désassembler, de décompiler et d'analyser le code exécutable pour comprendre son fonctionnement.

11. Conclusion

Nous pouvons conclure que le format PE est un format de fichier exécutable spécifique à Windows. Il est utilisé pour stocker les fichiers binaires exécutables et les bibliothèques de liens dynamiques (.exe, .dll, .ocx, .scr, etc.).

Le format PE contient des informations importantes sur la structure du fichier, telles que la signature HEXA, le TimeDateStamp, et les Sections qui composent le fichier.

Le format PE est utilisé principalement sur les systèmes d'exploitation Windows, mais il peut également être utilisé sur d'autres systèmes, comme Wine sur Linux. Si Windows ne reconnaît pas le format PE pour un fichier, cela signifie que le fichier ne peut pas être exécuté sur ce système.

Le format PE est analysé à l'aide de logiciels tels que PE Explorer, IDA Pro, OllyDbg, ou encore WinDbg. Ces logiciels permettent d'analyser les fichiers PE pour en extraire des informations utiles, telles que le code du programme, les Sections, ou encore les packers utilisés.

Enfin, les packers sont des outils utilisés pour compresser, crypter ou modifier les fichiers exécutables afin de les rendre plus difficiles à analyser ou à décompiler.

12. Glossaire

PE : Portable Executable, format de fichier binaire pour les fichiers exécutables Windows.

Extensions de fichiers : .cpl, .exe, .dll, .ocx, .sys, .scr, .drv, .efi.

Signature HEXA : "4D 5A", qui correspond aux lettres "MZ" en ASCII.

SE : Système d'exploitation.

TimeStamp : Correspond à la date de compilation ou de liaison de l'exécutable.

Sections : Les sections couramment trouvées dans un fichier PE sont : .text, .rdata, .data, .rsrc, .idata, .reloc, .debug, .tls.

Packer : Petit programme qui permet de compresser et d'encoder un fichier binaire afin de le rendre plus petit et plus difficile à analyser, à déboguer ou à désassembler.