

# TP 5 Guillaume Sanchez

## Rédigez un résumé explicatif et visuel du format PE

Le format PE veut dire portable exécutable. Comme son nom l'indique, il s'agit d'un format de fichiers qui peut être exécuter sans installation car il regroupe ou exploite les exécutables et les bibliothèques présent sur le système d'exploitation.

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

Plusieurs extensions peuvent être des PE, le .exe, le ocx, le .dll, le .cpl ou encore le .efi.

## Quelle signature HEXA le format PE prend-il ?

La signature au format HEXA est "4D 5A"

## Sous quels SE retrouve-t-on le format PE ?

On retrouve le sur Windows 32 bit et 64 bits.

## Que se passe t-il si Windows ne reconnait pas le format PE pour le fichier ?

Plusieurs comportements peuvent être observer lorsque windows ne reconnait pas le format PE d'un fichier. Un message d'erreur peut apparaitre ou un avertissement de sécurité. Une fenêtre de dialogue pour choisir un programme peut s'ouvrir pour permettre de l'exécuter. Potentiellement il ne peut également rien se passer.

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

On peut le retrouver dans L'en-tête PE, plus particulièrement dans dans le FileHeader :

```
typedef struct _IMAGE_FILE_HEADER {  
    WORD Machine;  
    WORD NumberOfSections;  
    DWORD TimeDateStamp;  
    DWORD PointerToSymbolTable;  
    DWORD NumberOfSymbols;  
    WORD SizeOfOptionalHeader;  
    WORD Characteristics;  
} IMAGE_FILE_HEADER, *PIMAGE_FILE_HEADER;
```

## A quoi cela correspond-il ?

Cela correspond à la date et à l'heure à laquelle le fichier a été créé ou compilé.

## Est-ce utile pour une analyse de fichier ?

Oui car cela permet de savoir si le fichier a été modifié ou corrompu. Si c'est le cas, le TimeDateStamp ne sera pas le même que celui du fichier d'origine.

## Combien peut-il y avoir de Section dans le format PE ?

Il n'y a pas réellement de limite de section dans le format PE bien que le maximum supporté par Windows soit de 96 sections. Pour des raisons pratiques, en général un fichier PE peut être limité à un nombre raisonnable afin qu'il ne soit pas trop lourd.

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

Au Format PE, le code du programme se trouve par défaut dans la section ".text".

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

Un packer est un outil utilisé pour compresser, chiffrer ou autrement modifier le contenu d'un fichier exécutable afin de réduire sa taille, de le protéger contre l'ingénierie inverse, ou de le rendre plus difficile à détecter par les logiciels antivirus. Les packers sont souvent utilisés dans le développement de logiciels légitimes pour réduire la taille des fichiers exécutables et protéger la propriété intellectuelle.

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

Il existe plusieurs logiciels qui permettent d'analyser un fichier au format PE, en voici 5 :

- PEiD
- PE Explorer
- CFF
- IDA Pro
- Ghidra