2021/02/24_PE_第7课_LoadPE、手写PE程序

笔记本:	PE
创建时间:	2021/2/24 星期三 10:24
作者:	ileemi

使用 "#pragma command("link", xxx)" 可以修改节的信息（section）

LoadPE

获取导入表的地址，导入表的地址在数据目录中，数据目录在选项头中。

判断导入表的名称是否为空（为空将IAT表当作名称表去解析），以及导出函数是否是序号导入（判断最高位是否为1，为1将高16位清0，低16位当做序号）。

可执行文件的入口地址在文件中的偏移可通选项头的 "**AddressOfEntryPoint**" 获取。基址可通过 "**ImageBase**" 获取。内存镜像大小可通过 "**SizeOfImage**" 获取。

手写PE

PE文件的文件对齐值在 "Win XP" 上可以给4，但是在 "Win7 和 Win10" 上PE文件对齐值最低要给200字节。

一个最小字节数可运行的PE文件需要手写16进制数据，还需要不同结构体的成员进行重复利用。