(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104679561 A
(43)申请公布日 2015.06.03

(21)申请号 201510081941.7

(22)申请日 2015.02.15

(71)申请人 福建天晴数码有限公司
地址 350000 福建省福州市福州开发区星发路8号生产力促进中心大厦三层301室

(72)发明人 刘德建 方振华 何巍巍 翁祖岚

(74)专利代理机构 福州市鼓楼区博深专利代理事务所(普通合伙) 35214
代理人 林志峥

(51)Int.Cl.
G06F 9/445(2006.01)

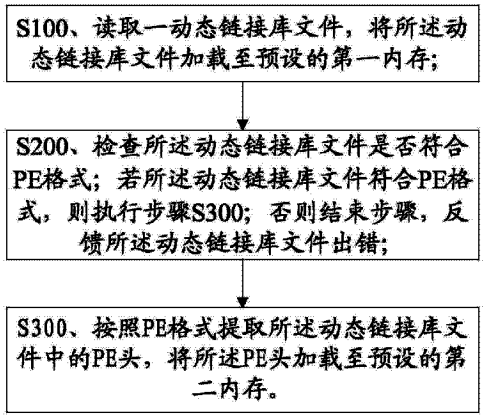
权利要求书1页 说明书5页 附图3页

(54)发明名称

一种动态链接库文件加载的方法及系统

(57)摘要

本发明涉及动态链接库领域，尤其涉及一种动态链接库文件加载的方法及系统。该方法包括：S100、读取一动态链接库文件，将所述动态链接库文件加载至预设的第一内存；S200、检查所述动态链接库文件是否符合PE格式；若所述动态链接库文件符合PE格式，则执行步骤S300；否则结束步骤，反馈所述动态链接库文件出错；S300、按照PE格式提取所述动态链接库文件中的PE头，将所述PE头加载至预设的第二内存。通过将符合PE格式的动态链接库文件加载至第一内存，再将所述动态链接库的PE头加载至第二内存，实现PE加载。



CN 104679561 A

1. 一种动态链接库文件加载的方法，其特征在于，包括以下步骤：

S100、读取一动态链接库文件，将所述动态链接库文件加载至预设的第一内存；

S200、检查所述动态链接库文件是否符合 PE 格式；若所述动态链接库文件符合 PE 格式，则执行步骤 S300；否则结束步骤，反馈所述动态链接库文件出错；

S300、按照 PE 格式提取所述动态链接库文件中的 PE 头，将所述 PE 头加载至预设的第二内存。

2. 根据权利要求 1 所述的动态链接库文件加载的方法，其特征在于，还包括步骤 S400、根据所述 PE 头更新基址信息，将所述动态链接库文件的节信息加载至预设的第二内存；调整重定位表，加载所需要的动态链接库文件的基址信息和调整导入表；根据节头标记内存页，节被标记为可丢弃。

3. 根据权利要求 1 所述的动态链接库文件加载的方法，其特征在于，该方法具体包括：

步骤 1、读一个目标 DLL 文件到内存；

步骤 2、内存加载目标 DLL 文件，具体包括：

步骤 21、检测目标 DLL 文件是否是正常的 PE 格式；

步骤 22、目标 DLL 文件为 PE 格式的文件，PE 头位于 PE 文件中的偏移的某个位置，为 DLL 的 PE 头分配以 MEM_COMMIT 标志的内存块；

步骤 23、把 PE 头拷贝到分配的内存块；

步骤 24、PE 头更新 imagebase 信息；

步骤 25、从目标 DLL 文件拷贝节信息到新分配的内存；

步骤 26、调整重定位表；

步骤 27、加载所需要的 dll 基址和调整导入表；

步骤 28、根据节头标记内存页，节被标记为可丢弃，进行释放。

4. 一种动态链接库文件加载的系统，其特征在于，包括读取单元、第一加载单元、检查单元、提取单元和第二加载单元；

所述读取单元，用于读取一动态链接库文件；

所述第一加载单元，用于将所述动态链接库文件加载至预设的第一内存；

所述检查单元，用于检查所述动态链接库文件是否符合 PE 格式；

所述提取单元，用于按照 PE 格式提取所述动态链接库文件中的 PE 头；

所述第二加载单元，用于将所述 PE 头加载至预设的第二内存。

一种动态链接库文件加载的方法及系统

技术领域

[0001] 本发明涉及动态链接库领域，尤其涉及一种动态链接库文件加载的方法及系统。

背景技术

[0002] 关于动态链接库文件的隐藏方法很多，如抹链的方法，可以让动态链接库文件从模块链表中消失，但是在 XT 等工具在驱动层中还是可以查找到动态链接库文件的踪迹，隐藏效果不好。所述 XT 为 XueTr，是一款广受好评的操作系统管理工具，有进程、线程、进程模块、进程窗口、进程内存信息查看、热键信息查看，杀进程、杀线程、卸载模块等功能。

[0003] (1) 远程线程注入方法主要有两种，一种是直接复制母体中预注入的代码到目标进程地址空间，然后启动注入的代码，这种远程线程一旦成功实现，那么它只出现在目标进程的内存中，并没有对应的磁盘文件，隐蔽性看起来不错，缺点就是，必须要在注入代码中对所有直接寻址的指令进行修正，然而采用汇编手动修改过于繁琐；

[0004] (2) 另一种更为常用的方法是注入一个 dll 文件到目标进程，这种方法的实现可以是以一个消息 Hook 为由进行注入，或者仍然使用代码，这种方法的优点是 dll 文件自带重定位表，也就是说你不必再为修正直接寻址指令而烦恼了，dll 自己会重定位！。但它的缺点就是可以用进程管理工具看见被加载的 dll 文件名、文件路径。这样就不太完美了，，因为只要用户看看模块列表很容易发现可疑模块，得到 dll 的全路径，dll 文件就这样暴露了。

发明内容

[0005] 本发明所要解决的技术问题是：提供一种无痕加载的动态链接库文件加载的方法及系统。

[0006] 为了解决上述技术问题，本发明采用的技术方案为：

[0007] 一种动态链接库文件加载的方法，包括以下步骤：

[0008] S100、读取一动态链接库文件，将所述动态链接库文件加载至预设的第一内存；

[0009] S200、检查所述动态链接库文件是否符合 PE 格式；若所述动态链接库文件符合 PE 格式，则执行步骤 S300；否则结束步骤，反馈所述动态链接库文件出错；

[0010] S300、按照 PE 格式提取所述动态链接库文件中的 PE 头，将所述 PE 头加载至预设的第二内存。

[0011] 本发明采用的另一技术方案为：

[0012] 一种动态链接库文件加载的系统，包括读取单元、第一加载单元、检查单元、提取单元和第二加载单元；

[0013] 所述读取单元，用于读取一动态链接库文件；

[0014] 所述第一加载单元，用于将所述动态链接库文件加载至预设的第一内存；

[0015] 所述检查单元，用于检查所述动态链接库文件是否符合 PE 格式；

[0016] 所述提取单元，用于按照 PE 格式提取所述动态链接库文件中的 PE 头；

[0017] 所述第二加载单元，用于将所述 PE 头加载至预设的第二内存。

[0018] 本发明的有益效果在于：

[0019] 1、通过本发明提供的加载方法，加载动态链接库文件比较隐蔽；因为其不是通过篡改 PEB(PEB 为进程环境块，是一个保存了进程的相关信息的结构体）中 LDR 链的信息，把需要隐藏的模块从 LDR 链表中摘除，达到隐藏的目地，而是直接把动态链接库文件加载到内存，没有留下任何踪迹，通过 OD 和 XT 工具都查不出踪迹；

[0020] 2、在 32 位和 64 位系统上通过此加载方法加载动态链接库文件比较稳定；

[0021] 3、有时游戏需要在 R3 应用层（Intel 的 CPU 将特权级别分为 4 个级别：RING0、RING1、RING2 和 RING3；Windows 只使用 RING0 和 RING3，RING0 只给操作系统用，RING3 可以给操作系统和应用层都能用）对动态链接库文件进行隐藏，防止被人利用找到动态链接库文件的句柄，对动态链接库文件进行非法操作；此加载方法可以实现让动态链接库文件加载基地址时不让外挂动态获取到。

附图说明

[0022] 图 1 为本发明具体实施方式的动态链接库文件加载的方法的流程图；

[0023] 图 2 为本发明具体实施方式的动态链接库文件加载的结构示意图；

[0024] 图 3 为本发明具体实施方式的 PE 文件结构图；

[0025] 图 4 为本发明具体实施方式的磁盘和内存中的 PE 文件结构对比图；

[0026] 标号说明：

[0027] 10、读取单元；20、第一加载单元；30、检查单元；40、提取单元；50、第二加载单元。

具体实施方式

[0028] 为详细说明本发明的技术内容、所实现目的及效果，以下结合实施方式并配合附图予以说明。

[0029] 本发明最关键的构思在于：通过将符合 PE 格式的动态链接库文件加载至第一内存，再将所述动态链接库的 PE 头加载至第二内存，实现 PE 加载。

[0030] 请参照图 1，为本发明具体实施方式的动态链接库文件加载的方法的流程图，具体如下：

[0031] 一种动态链接库文件加载的方法，包括以下步骤：

[0032] S100、读取一动态链接库文件，将所述动态链接库文件加载至预设的第一内存；

[0033] S200、检查所述动态链接库文件是否符合 PE 格式；若所述动态链接库文件符合 PE 格式，则执行步骤 S300；否则结束步骤，反馈所述动态链接库文件出错；

[0034] S300、按照 PE 格式提取所述动态链接库文件中的 PE 头，将所述 PE 头加载至预设的第二内存。

[0035] 从上述描述可知，本发明的有益效果在于：

[0036] 1、通过本发明提供的加载方法，加载动态链接库文件比较隐蔽；因为其不是通过篡改 PEB(PEB 为进程环境块，是一个保存了进程的相关信息的结构体）中 LDR 链的信息，把需要隐藏的模块从 LDR 链表中摘除，达到隐藏的目地，而是直接把动态链接库文件加载到内存，没有留下任何踪迹，通过 OD 和 XT 工具都查不出踪迹；

[0037] 2、在 32 位和 64 位系统上通过此加载方法加载动态链接库文件比较稳定；

[0038] 3、有时游戏需要在 R3 应用层（Intel 的 CPU 将特权级别分为 4 个级别：RING0、RING1、RING2 和 RING3；Windows 只使用 RING0 和 RING3，RING0 只给操作系统用，RING3 可以给操作系统和应用层都能用）对动态链接库文件进行隐藏，防止被人利用找到动态链接库文件的句柄，对动态链接库文件进行非法操作；此加载方法可以实现让动态链接库文件加载基地址时不让外挂动态获取到。

[0039] 进一步的，还包括步骤 S400、根据所述 PE 头更新基址信息，将所述动态链接库文件的节信息加载至预设的第二内存；调整重定位表，加载所需要的动态链接库文件的基址信息和调整导入表；根据节头标记内存页，节被标记为可丢弃。

[0040] 进一步的，所述步骤 S300 具体为：按照 PE 对齐的方式（PE 装载器将 PE 文件装入内存，每个 PE 节区以 1000 为对齐，改变各个节区的偏移地址。通常，一个 PE 文件在磁盘上的映像跟内存中的基本一致，但并不是完全的拷贝。Windows 加载器会决定哪些部分需要加载，哪些部分不需要加载，而且由于磁盘对齐与内存对齐的不一致，加载到内存的 PE 文件与磁盘上的 PE 文件各个部分的分布都会有差异。）将所述 PE 头加载至预设的第二内存。按 PE 对齐的方式加载是一个正常的处理流程，需要这样才能让代码加载正确并可执行。

[0041] 进一步的，该方法具体包括：

[0042] 步骤 1、读一个目标 DLL 文件到内存；

[0043] 步骤 2、内存加载目标 DLL 文件，具体包括：

[0044] 步骤 21、检测目标 DLL 文件是否是正常的 PE 格式；

[0045] 步骤 22、目标 DLL 文件为 PE 格式的文件，PE 头位于 PE 文件中的偏移的某个位置，为 DLL 的 PE 头分配以 MEM_COMMIT 标志的内存块；

[0046] 步骤 23、把 PE 头拷贝到分配的内存块；

[0047] 步骤 24、PE 头更新 imagebase 信息；

[0048] 步骤 25、从目标 DLL 文件拷贝节信息到新分配的内存；

[0049] 步骤 26、调整重定位表；

[0050] 步骤 27、加载所需要的 dll 基址和调整导入表；

[0051] 步骤 28、根据节头标记内存页，节被标记为可丢弃，进行释放。

[0052] 请参阅图 2，为本发明具体实施方式的动态链接库文件加载的结构示意图，具体如下：

[0053] 一种动态链接库文件加载的系统，包括读取单元 10、第一加载单元 20、检查单元 30、提取单元 40 和第二加载单元 50；

[0054] 所述读取单元 10，用于读取一动态链接库文件；

[0055] 所述第一加载单元 20，用于将所述动态链接库文件加载至预设的第一内存；

[0056] 所述检查单元 30，用于检查所述动态链接库文件是否符合 PE 格式；

[0057] 所述提取单元 40，用于按照 PE 格式提取所述动态链接库文件中的 PE 头；

[0058] 所述第二加载单元 50，用于将所述 PE 头加载至预设的第二内存。

[0059] 从上述描述可知，本发明的有益效果在于：

[0060] 1、通过本发明提供的加载方法，加载动态链接库文件比较隐蔽；因为其不是通过篡改 PEB（PEB 为进程环境块，是一个保存了进程的相关信息的结构体）中 LDR 链的信息，把

需要隐藏的模块从 LDR 链表中摘除，达到隐藏的目地，而是直接把动态链接库文件加载到内存，没有留下任何踪迹，通过 OD 和 XT 工具都查不出踪迹；

[0061] 2、在 32 位和 64 位系统上通过此加载方法加载动态链接库文件比较稳定；

[0062] 3、有时游戏需要在 R3 应用层（Intel 的 CPU 将特权级别分为 4 个级别：RING0、RING1、RING2 和 RING3；Windows 只使用 RING0 和 RING3，RING0 只给操作系统用，RING3 可以给操作系统和应用层都能用）对动态链接库文件进行隐藏，防止被人利用找到动态链接库文件的句柄，对动态链接库文件进行非法操作；此加载方法可以实现让动态链接库文件加载基地址时不让外挂动态获取到。

[0063] 如图 3,4 所示，本发明的实施例一为：

[0064] 1、读一个目标 DLL 文件到内存：LPVOIDlpMem = ReadFileToMem(szDllFile)；

[0065] 2、内存直接加载 DLL：MemoryLoadLibrary(lpMem)；

[0066] (1) 检查目标 DLL 是否是正常的 PE 格式；

[0067] (2)DLL 为 PE 格式的文件，PE 头位于 PE 文件中的偏移的某个位置，为 DLL 的 PE 头分配以 MEM_COMMIT 标志的内存块；

[0068] (3) 把 PE 头拷贝到分配的内存块；

[0069] 具体为：读入 PE 文件的 PE 头，包括 DOS 头、PE 头和 Section 头，到新分配的内存块；

[0070] (4)PE 头更新 imageBase 信息；

[0071] 具体为：windows 加载器根据 PE 头里的 ImageBase 所定义的加载地址是否可用，如果已被其他模块占用，则重新分配一块空间；如果文件被加载的地址不是 ImageBase 定义的地址，则重新修正 ImageBase。

[0072] (5) 从 DLL 文件拷贝节信息到新分配的内存；

[0073] 具体为：根据节头部的信息，把文件的各个节映射到分配的空间，并根据各个节定义的数据来修改所映射的页的属性。

[0074] (6) 调整重定位表；

[0075] 具体为：针对直接寻址的指令需要修复重定位表，否则寻址会失败。程序加载器所作的重定位工作，就是将程序中需要重定位的地方，都加上程序的加载地址。

[0076] (7) 加载所需要的 d11 基址和调整导入表；

[0077] 具体为：根据 PE 文件的输入表加载所需要的 DLL 到进程空间，然后替换 IAT 表内的数据为实际调用函数的地址。

[0078] (8) 根据节头标记内存页，节被标记为可丢弃的要释放掉。

[0079] 综上所述，本发明提供的一种动态链接库文件加载的方法及系统；通过本发明提供的加载方法，加载动态链接库文件比较隐蔽；因为其不是通过篡改 PEB(PEB 为进程环境块，是一个保存了进程的相关信息的结构体）中 LDR 链的信息，把需要隐藏的模块从 LDR 链表中摘除，达到隐藏的目地，而是直接把动态链接库文件加载到内存，没有留下任何踪迹，通过 OD 和 XT 工具都查不出踪迹；在 32 位和 64 位系统上通过此加载方法加载动态链接库文件比较稳定；有时游戏需要在 R3 应用层（Intel 的 CPU 将特权级别分为 4 个级别：RING0、RING1、RING2 和 RING3；Windows 只使用 RING0 和 RING3，RING0 只给操作系统用，RING3 可以给操作系统和应用层都能用）对动态链接库文件进行隐藏，防止被人利用找到动态链接

库文件的句柄，对动态链接库文件进行非法操作；此加载方法可以实现让动态链接库文件加载基地址时不让外挂动态获取到。

[0080] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等同变换，或直接或间接运用在相关的技术领域，均同理包括在本发明的专利保护范围内。

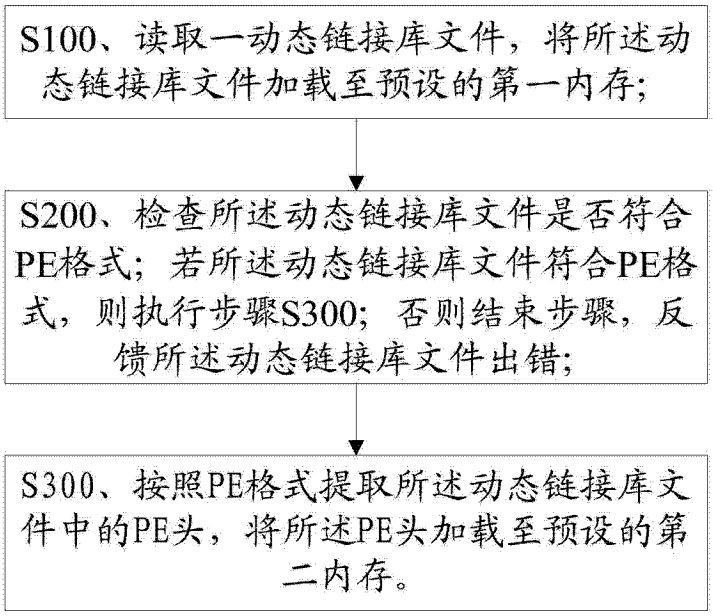

S100、读取一动态链接库文件，将所述动态链接库文件加载至预设的第一内存;
S200、检查所述动态链接库文件是否符合PE格式；若所述动态链接库文件符合PE格式，则执行步骤S300；否则结束步骤，反馈所述动态链接库文件出错;
S300、按照PE格式提取所述动态链接库文件中的PE头，将所述PE头加载至预设的第二内存。

图 1

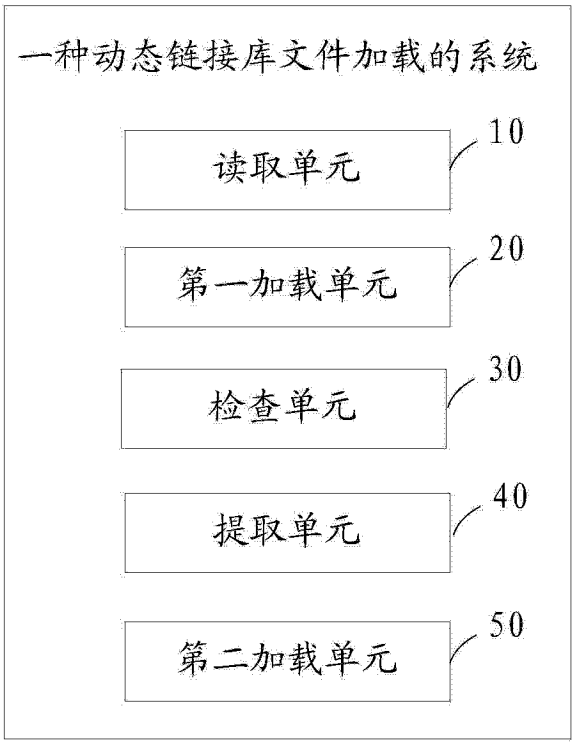

一种动态链接库文件加载的系统
读取单元
10
第一加载单元
20
检查单元
30
提取单元
40
第二加载单元
50

图 2

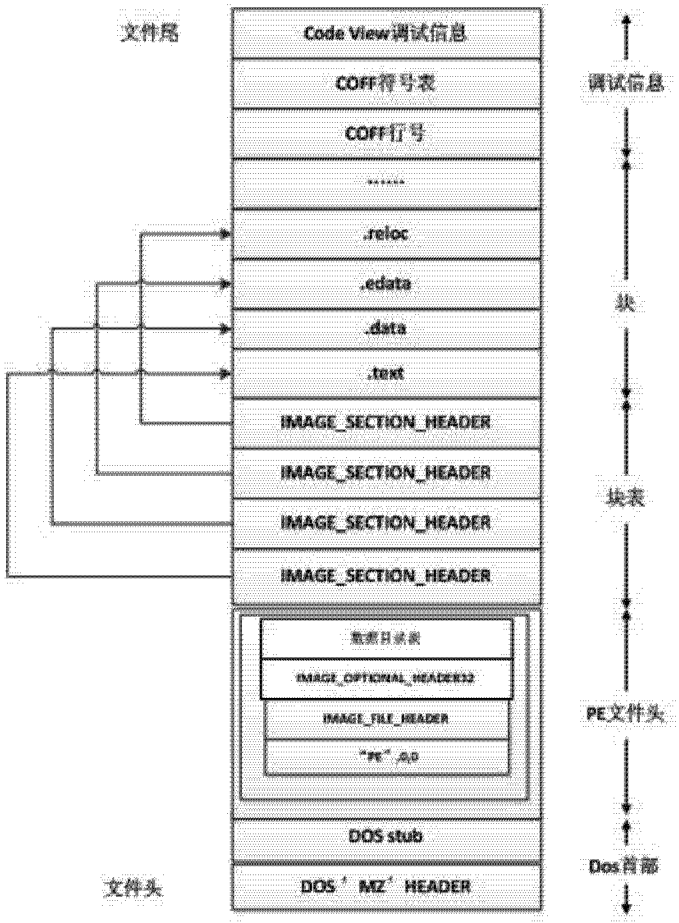

文件尾
Code View调试信息
COFF符号表
COFF行号
.....
.reloc
.edata
.data
.text
IMAGE_SECTION_HEADER
IMAGE_SECTION_HEADER
IMAGE_SECTION_HEADER
IMAGE_SECTION_HEADER
数据目录表
IMAGE_OPTIONAL_HEADER32
IMAGE_FILE_HEADER
"PE" 0,0
DOS stub
文件头
DOS 'MZ' HEADER
调试信息
块
块表
PE文件头
Dos首部

图 3

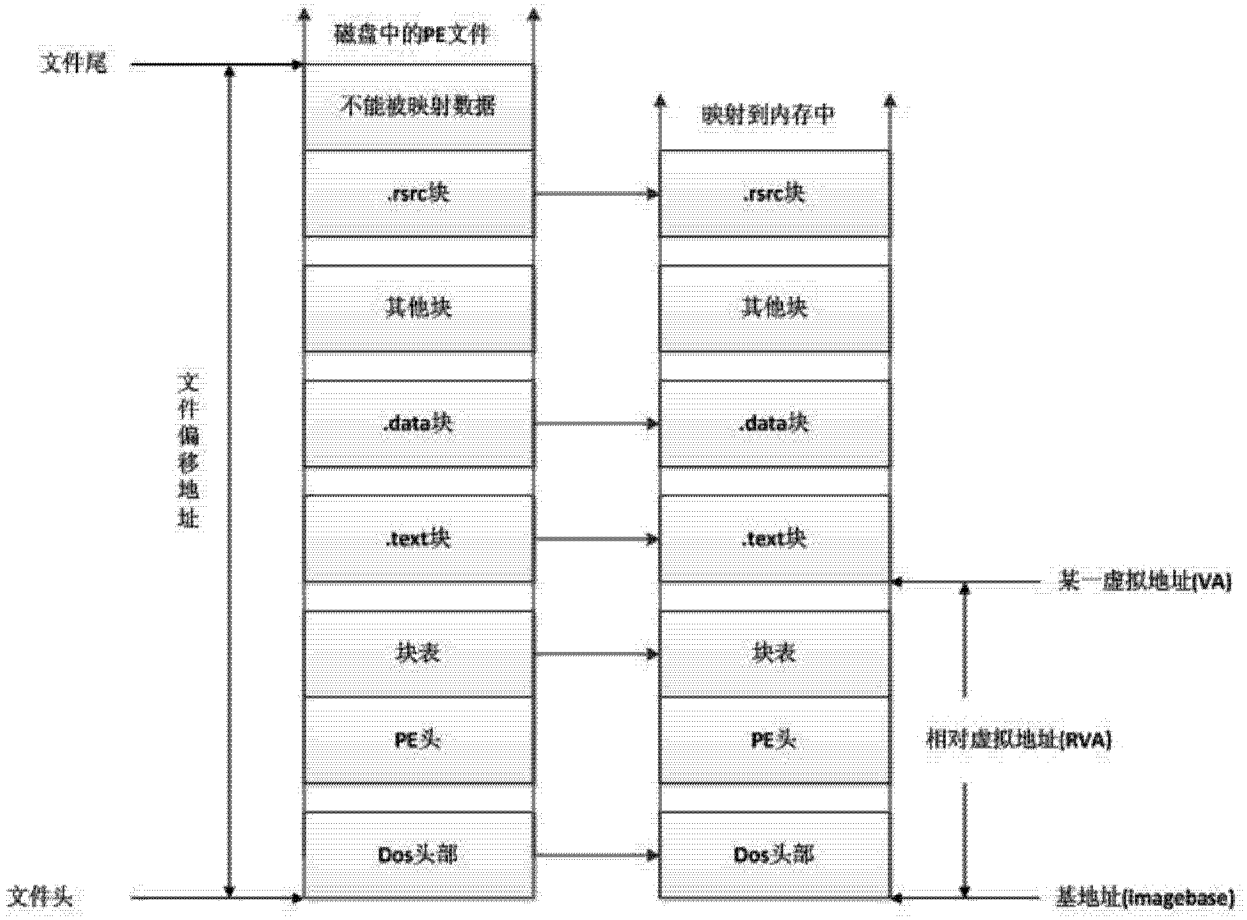

磁盘中的PE文件
文件尾
不能被映射数据
.rsrc块
其他块
.data块
.text块
块表
PE头
Dos头部
文件头
文件偏移地址
映射到内存中
.rsrc块
其他块
.data块
.text块
块表
PE头
Dos头部
某一虚拟地址(VA)
相对虚拟地址(RVA)
基地址(imagebase)

图 4