### PE手工缩小过程文档及缩减理由

1.0版

2017301110022 黄杨锋慧

1. 对初始760文件进行可修改部分尝试的结果：

|  |  |
| --- | --- |
| magic | 不可修改 |
| Major link version | 可修改 |
| Minor link version | 可修改 |
| Major Subsystem version | 不可修改 |
| Size of Image | 不可修改 |
| Size of Headers | 不可修改 |
| Subsystem | 不可修改 |
| DLL Characteristics | 不可修改 |
| CHECKSUM | 不可修改 |

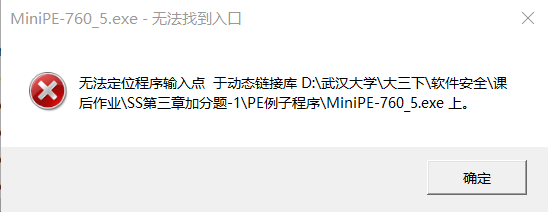
|  |  |
| --- | --- |
| Import table RVA | 不可修改 |
| Import table Size | 不可修改 |
| Resource table RVA | 不可修改 |
| TLS table RVA | 不可修改 |
| Load Configuration Table RVA | 不可修改 |
| COM+ Runtime Header RVA | 不可修改 |

|  |  |
| --- | --- |
| Virtual Size | 不可修改 |
| RVA | 不可修改 |
| Size of Raw data | 不可修改 |
| Offset to raw data | 不可修改 |

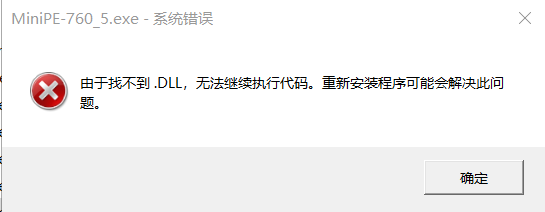
IAT可修改

IDT不可修改

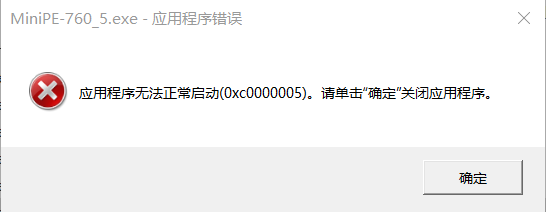
修改INT RVA的结果



修改Name RVA的结果



IAT RVA可以在一定范围内修改，但过大就会报错



INT

Hint/Name RVA不可修改

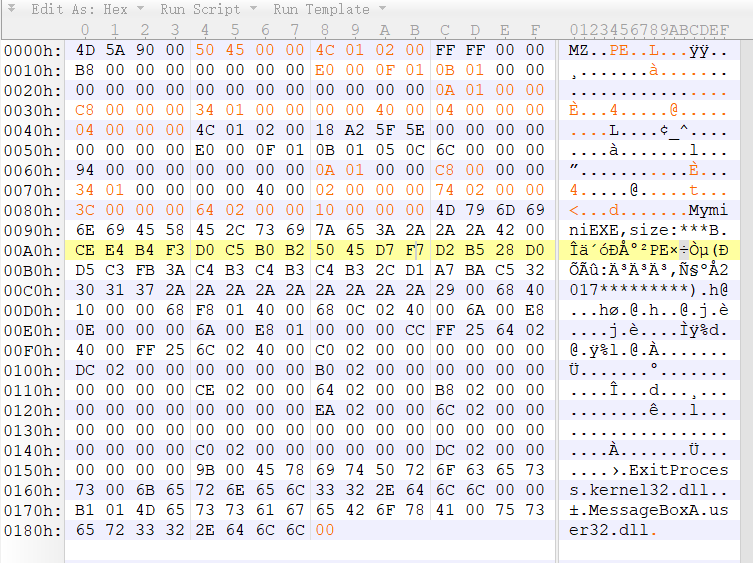


End of imports不可修改



1. 根据测试结果删去可初步删除的部分

* Dos stub
* Data directory保留两项——保留至输入表即可（import table）
* 节表删除
* PE文件头与MZ合并（注意相对位置）



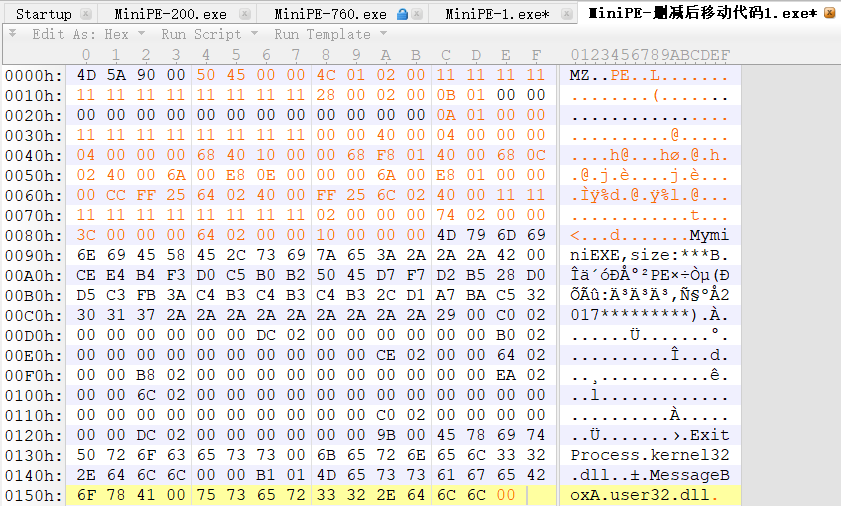
PS.关于0002的补充——可执行



|  |  |  |
| --- | --- | --- |
| FillCharacteristics | 文件特征值 | 指示文件属性的标志。参考3.2.2节“[特征](http://blog.csdn.net/qiming_zhang/article/details/7309909" \l "3.2.2)”。 |



* 将代码部分插缝进入可选文件头的可修改部分

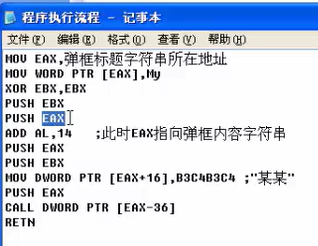


由于时间原因，在win10下的缩减还没有全部完成。

之后决定将xp下的200版本研究透并稍作修改，以方便之后在win10上进行修改。

1. 对200字节文件深入分析及实现

* 程序执行流程



* PE文件分析

4D 5A 00 00 50 45 00 00 4C 01 01 00 B8 86 00 40

MZ PE X86 1个节

00 66 C7 00 4D 79 EB 64 28 00 02 00 0B 01 4D 65

可选文件头大小28字节 Magic

02是指可执行

73 73 61 67 65 42 6F 78 41 00 00 00 0C 00 00 00

MessageBoxA Address of Entry Point

55 53 45 52 33 32 00 00 00 00 40 00 04 00 00 00

User32 Image Base Section Alignment

（INT RVA）

04 00 00 00 30 00 00 00 64 00 00 00 04 00 00 00

File Alignment Name RVA（dll） IAT RVA Major Subsystem version（不可修改）

0C 00 00 00 50 EB 15 00 0C 00 00 00 00 00 00 00

Win32 Version Value （Size of Image） Size of Header Checksum

02 00 00 00 1C 00 00 00 00 00 00 00 53 C7 40 16

Subsystem MessageBoxA ??????????

DLL Characteristics dll names

（不可修改）

C4 B3 C4 B3 FF 50 CA C3 02 00 00 00 33 DB 53 50

Data Directory

04 14 EB D0 38 00 00 00 6D 69 6E 69 45 58 45 2C

Import table RVA

指的是IDT

73 69 7A 65 3A 32 30 30 42 00 CE E4 B4 F3 D0 C5

B0 B2 50 45 D7 F7 D2 B5 28 D0 D5 C3 FB 3A C4 B3

00 00 00 00 2C D1 A7 BA C5 3A 32 30 31 31 33 30

后被赋值为“某某”

32 35 33 30 30 2A 2A 29

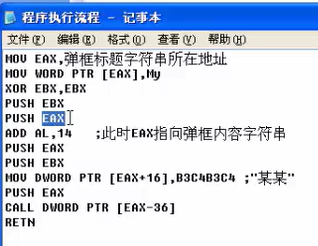
■代码

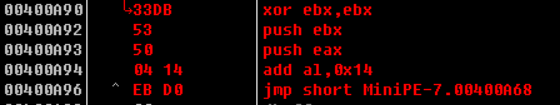
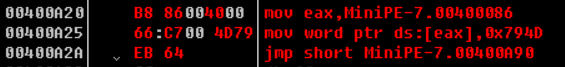
■数据

■固定位置的不可移动部分

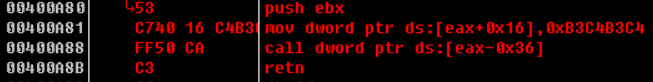
□不懂的部分

* 代码执行情况（Ollydbg）

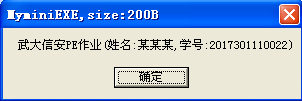








* 运行效果



在winXP下成功运行。