回忆杀-特征码免杀实践

原创 Uknow 零队 今天

注：这个是很久之前写的了

前言

前段时间，小马哥做了免杀的分享。其中就有说到特征码免杀，看到小马哥说的几个特征码定位的工具，我有种莫名的熟悉感。其中的MyCll这个工具名字可能不记得了，但是这个工具上面的狗熊logo异常的熟悉。

CCL与MYCCL都采用文件分块定位的办法，定位效果带有运气成份，且可能每次定位出的位置都不尽相同，这个免杀带来了困难。

VirTest5.0

小马哥介绍的是这款工具，下面是作者自己的介绍：

> 我们可以这样假设报毒过程，如果检测文件是PE,如果在CODE位置存在 标志A,在DATA位置存在标志B,在资源位置存在标志C,同时满足这个3个条件，那么杀软就会报毒,VIRTEST工作原理就是要找到引起报毒最后一个标志，也就是假设中的标志C。
>
> 因此VIRTEST采用2分排除法，测试标志C所在文件中的位置，由于被杀的文件可能存在多个 类似于ABC这样的连锁条件，所以我们必须要通过一种排除机制，先要找最靠近文件前部的连锁条件，排除掉文件尾部数据，当找到第一个连锁条件后，抹掉引标志C，再恢复尾部数据，
>
> 然后继续测试另外的连锁条件，直到找到最后一个连锁条件，抹掉后，整个文件免杀了，则说明特征代码被定位完毕了，所以VIRTEST绝对可以精确的定位出所有的复合特征。这比文件分块定位法先进得多，更为科学

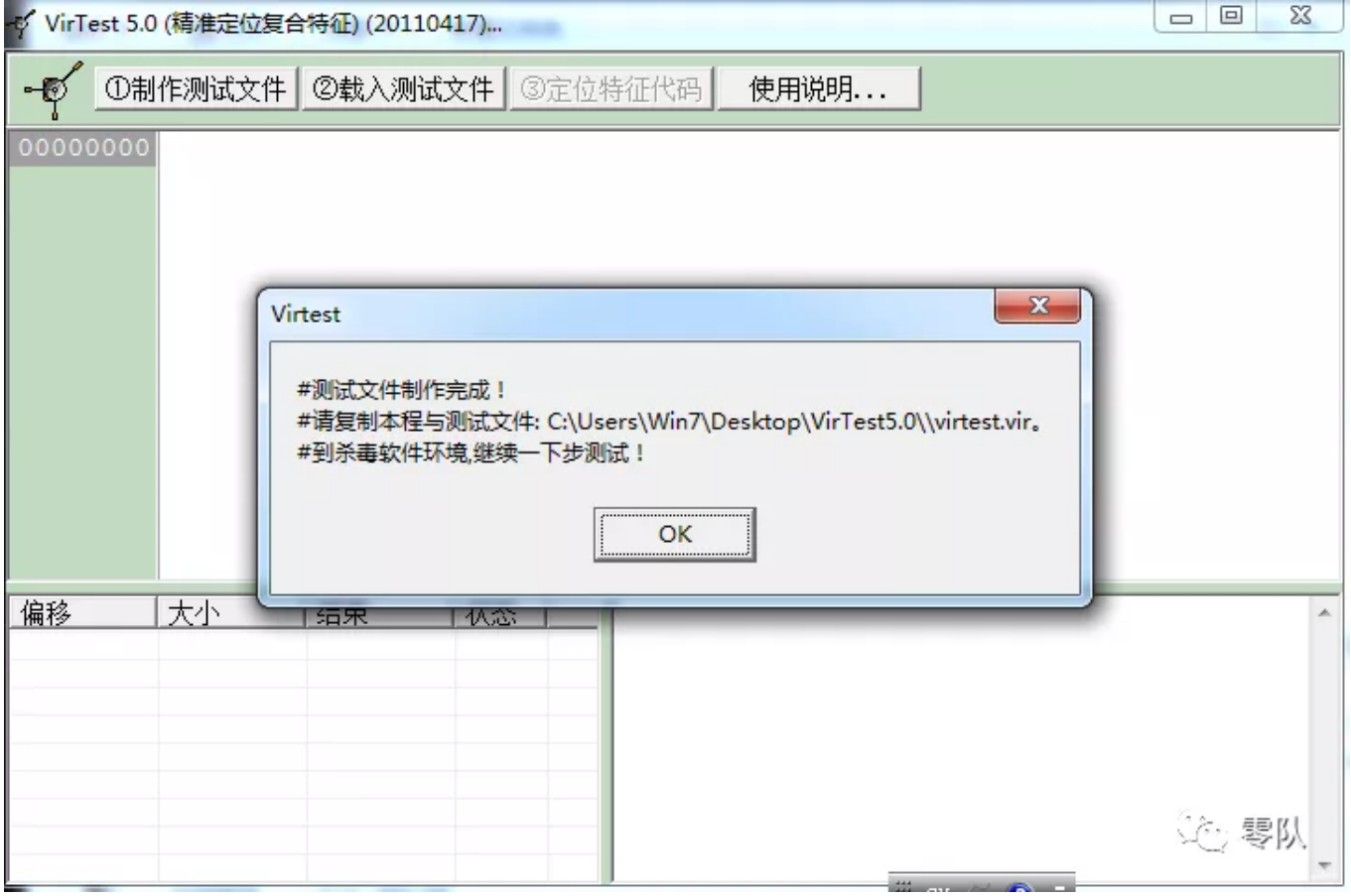
实践

这里我们选择一个功能比较简单的工具，如下ms15-051提权exp。选功能简单的工具主要原因：复杂功能的工具特征码特别多，且特征码修改后可能会影响工具的使用。

原有的ms15-051提权exp，在360全引擎最新病毒库的情况下是报毒的（建议断网）。

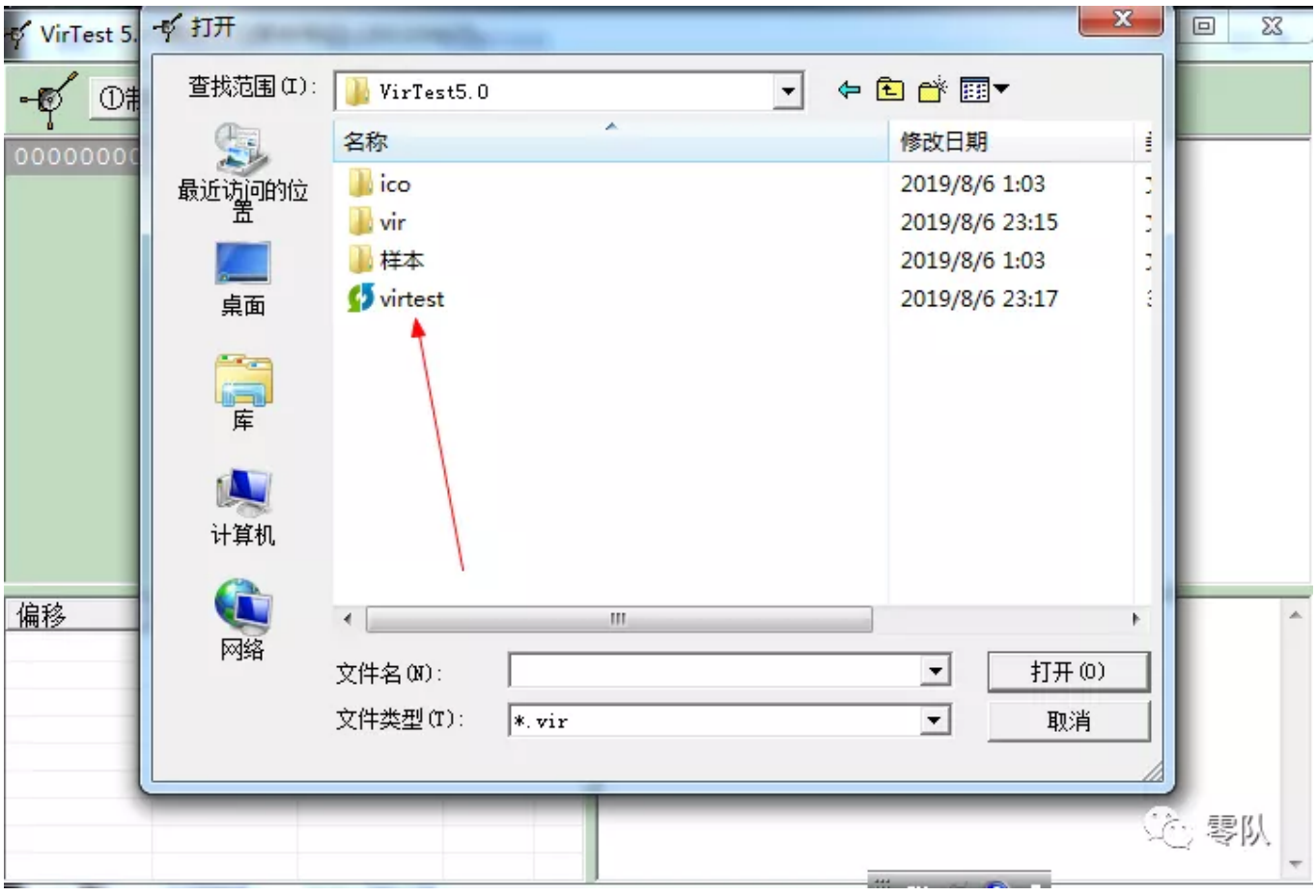
制作测试文件

首先点击“制作测试文件”导入ms15-051.exe。



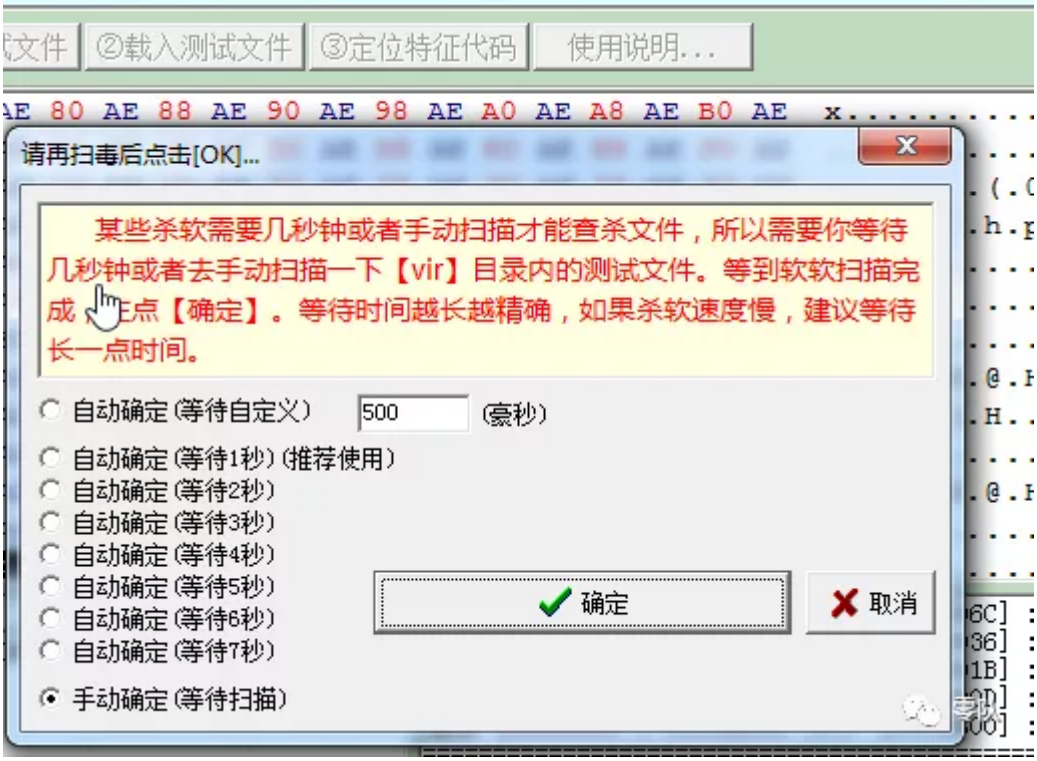
载入测试文件

然后载入上面图中说的生成文件virtest测试文件。

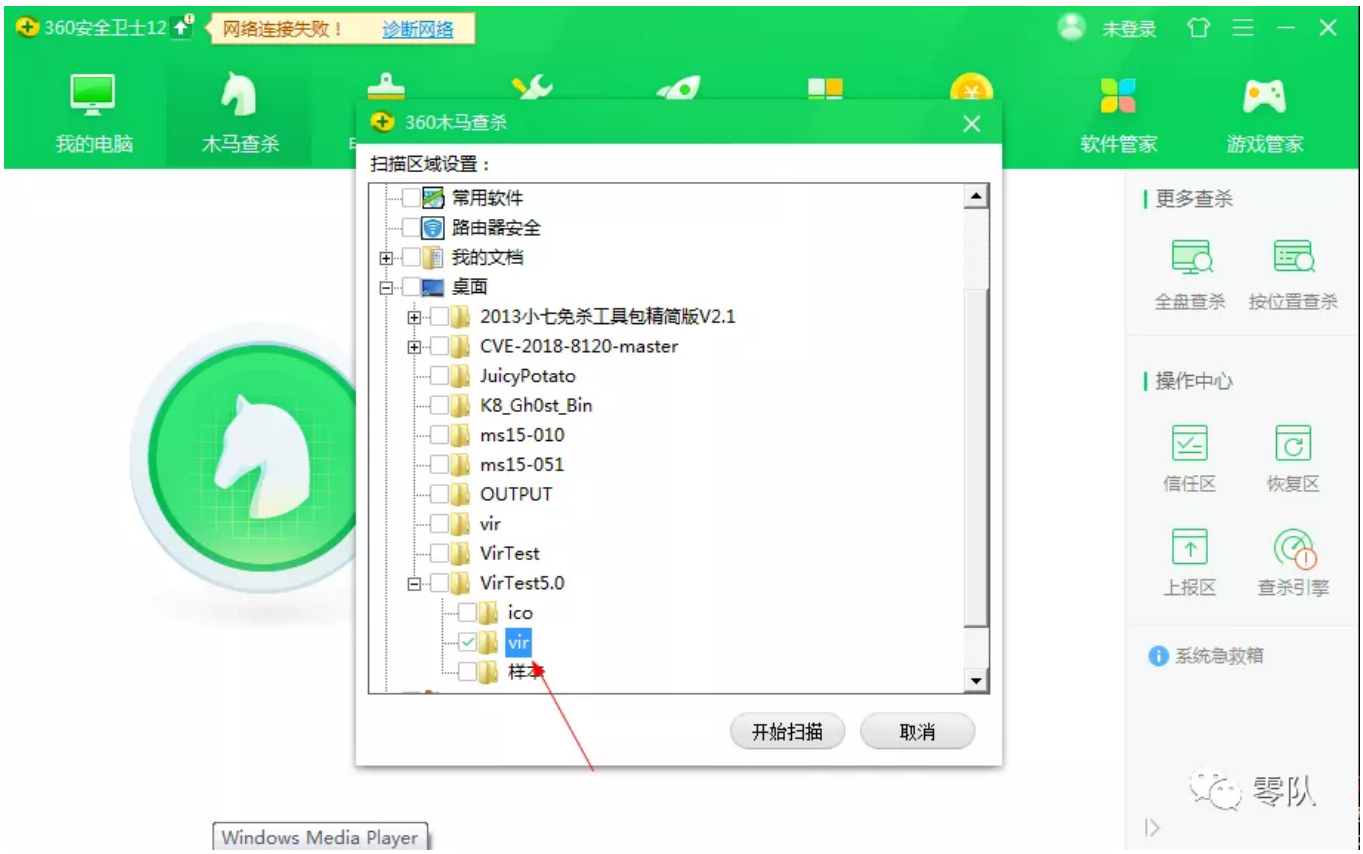


定位特征代码

再进行特征码定位



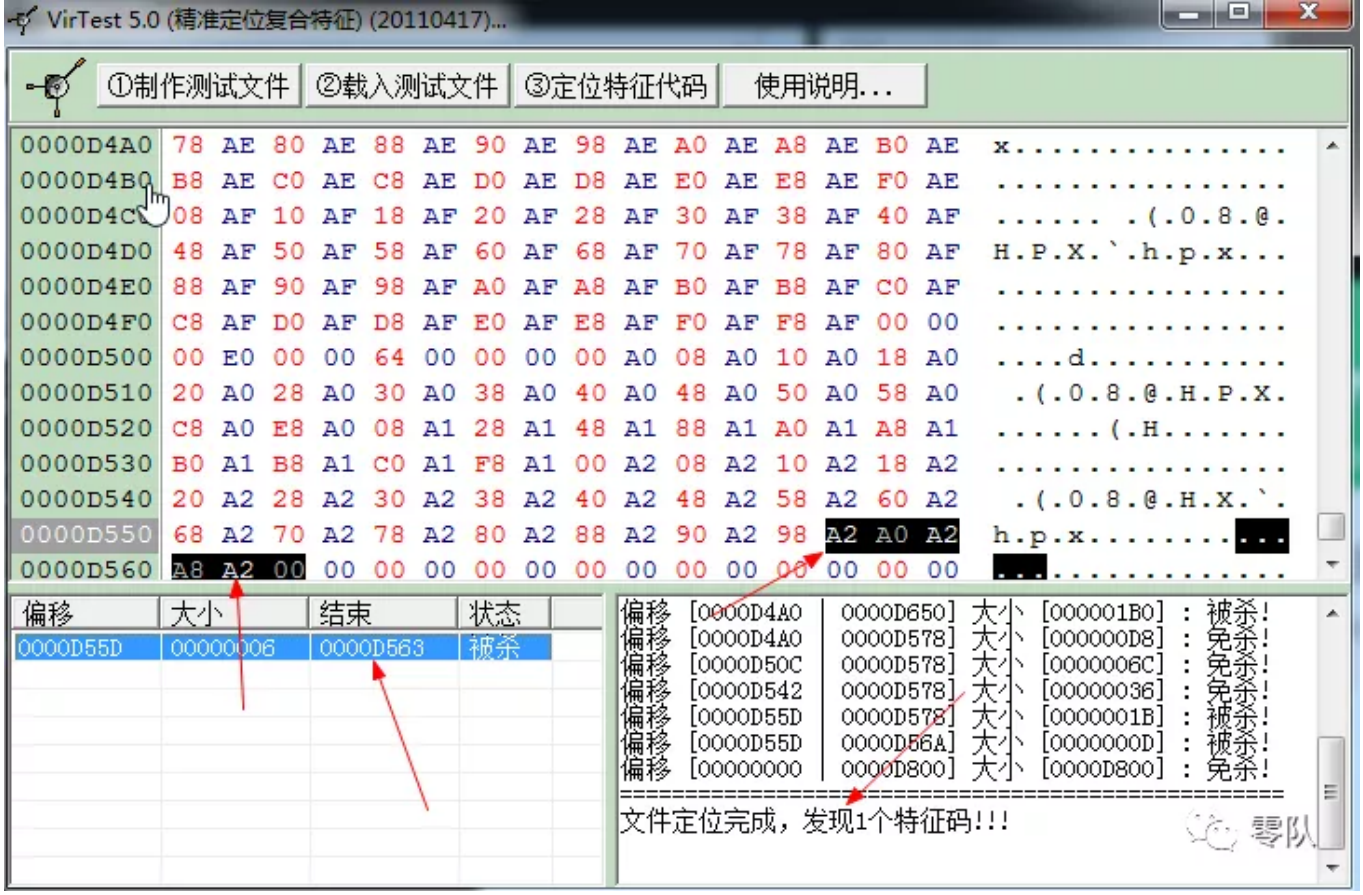
安装上面的提示对vir目录进行杀毒操作。



查杀vir目录生成文件，如查杀出病毒点击处理，再回到virtest点确定。

重复定位特征码，vir目录查杀。直到virtest提示已经找到特征码。

```
 1.==================================================
 2.偏移 [00000000 | 0000D800] 大小 [0000D800] : 被杀!
 3.偏移 [00000000 | 0000D800] 大小 [0000D800] : 免杀!
 4.偏移 [00006C00 | 0000D800] 大小 [00006C00] : 免杀!
 5.偏移 [0000A200 | 0000D800] 大小 [00003600] : 免杀!
 6.偏移 [0000BD00 | 0000D800] 大小 [00001B00] : 免杀!
 7.偏移 [0000CA80 | 0000D800] 大小 [00000D80] : 免杀!
 8.偏移 [0000D140 | 0000D800] 大小 [000006C0] : 免杀!
 9.偏移 [0000D4A0 | 0000D800] 大小 [00000360] : 被杀!
10.偏移 [0000D4A0 | 0000D650] 大小 [000001B0] : 被杀!
11.偏移 [0000D4A0 | 0000D578] 大小 [000000D8] : 免杀!
12.偏移 [0000D50C | 0000D578] 大小 [0000006C] : 免杀!
13.偏移 [0000D542 | 0000D578] 大小 [00000036] : 免杀!
14.偏移 [0000D55D | 0000D578] 大小 [0000001B] : 被杀!
15.偏移 [0000D55D | 0000D56A] 大小 [0000000D] : 被杀!
16.偏移 [00000000 | 0000D800] 大小 [0000D800] : 免杀!
17.==================================================
18.文件定位完成，发现1个特征码!!!
```



找到了特征码，只需要对这些地址进行修改就行了。

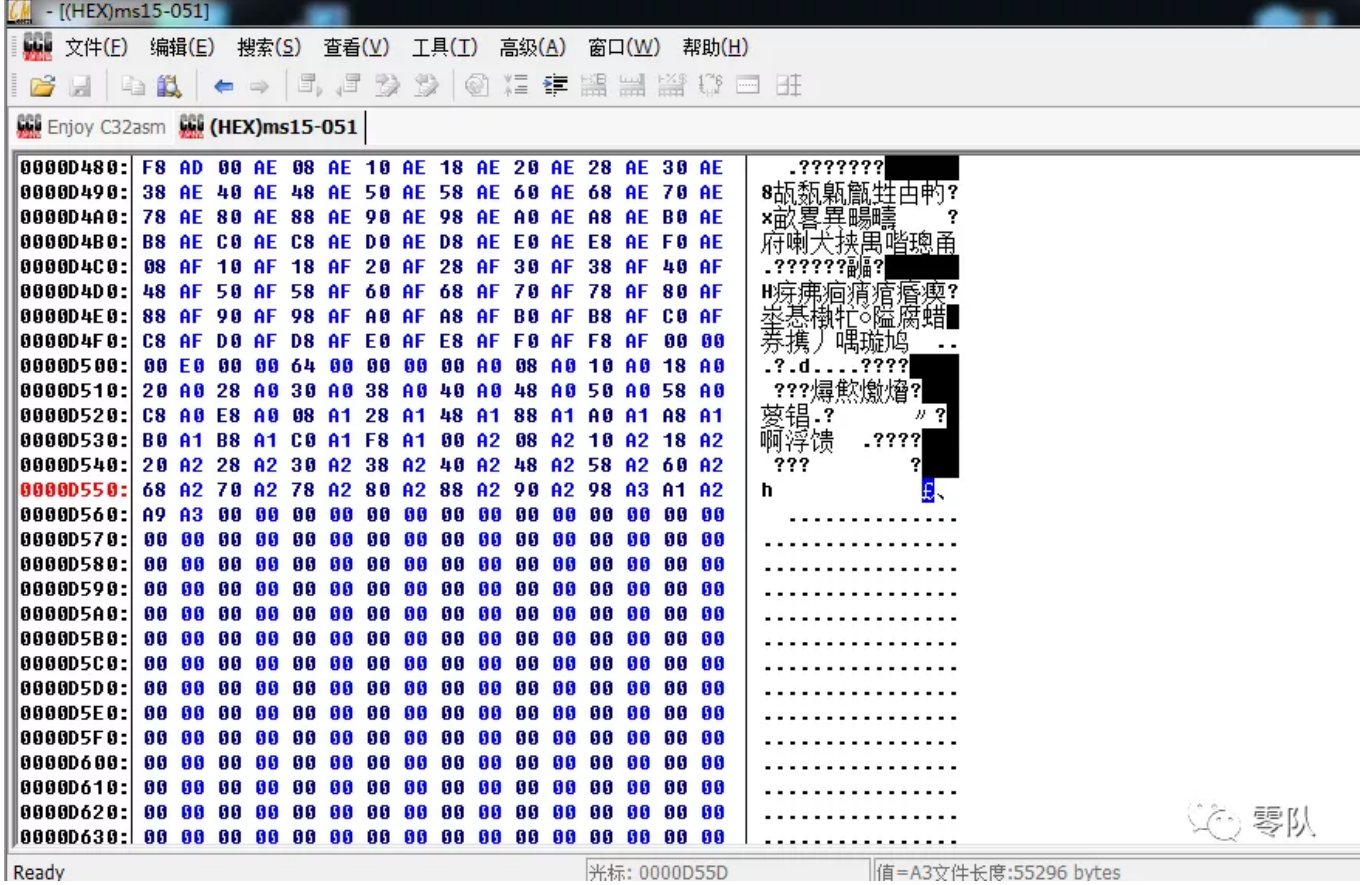
常用的修改工具有，OD，C32ASM，UE，010Editor等等。

修改特征代码

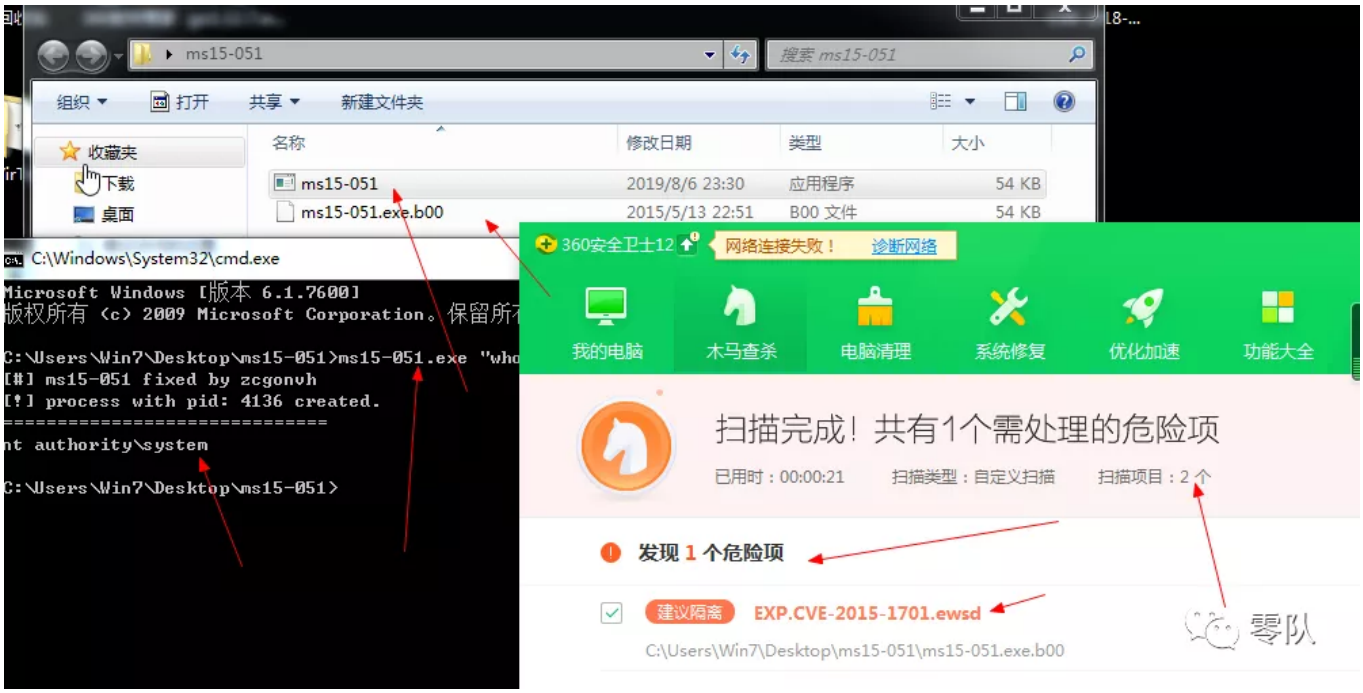
找到相应的地址。进行修改，引用《2019补天白帽大会》 ——Red Teaming 红队行动中《仙果：红队行动，攻防之杀毒软件对抗》的分享中的一句话。

> 之前学破解的时候有一个顺口溜，叫“74“变“75“， “84“变“85”，很老的一个段子。

如下图我们直接对特征码进行加1操作。



保存，会对旧文件进行备份，如下图中的ms15-051.exe.b00即备份文件。对ms15-051目录进行查杀，新生成的文件免杀且功能正常，可以进行提权操作。



附修改特征码方法

如下修改特征码的方法：（收集自网络）

- 直接修改特征码的十六进制法

  修改方法:把特征码所对应的十六进制改成数字差1或差不多的十六进制.

  适用范围:一定要精确定位特征码所对应的十六进制,修改后一定要测试一下能否正常使用.

- 修改字符串大小写法
  修改方法:把特征码所对应的内容是字符串的,只要把大小字互换一下就可以了.
  适用范围:特征码所对应的内容必需是字符串,否则不能成功.

- 等价替换法
  修改方法:把特征码所对应的汇编指令命令中替换成功能类拟的指令.
  适用范围:特征码中必需有可以替换的汇编指令.比如JN,JNE 换成JMP等.如果和我一样对汇编不怎们精通的可以去查查8080汇编手册.

- 指令顺序调换法
  修改方法:把具有特征码的代码顺序互换一下.
  适用范围:具有一定的局限性,代码互换后要不能影响程序的正常执行

- 通用跳转法
  修改方法:把特征码移到零区域(指代码的空隙处),然后一个JMP又跳回来执行.
  适用范围:没有什么条件,是通用的改法,强烈建议大家要掌握这种改法.