使用 file 命令，strings 命令，以及文件脱壳器等对恶意程序 RaDa.exe 进行基本检测

说明：由于 file 命令和 strings 命令是 Linux 命令，在 windows 下可使用 cygwin(www.cygwin.com)进行对 Linux 命令的模拟，或者下载专用的为 windows 使用的 file 和 strings 库

1. 使用 file 命令查看 RaDa.exe 的文件类型

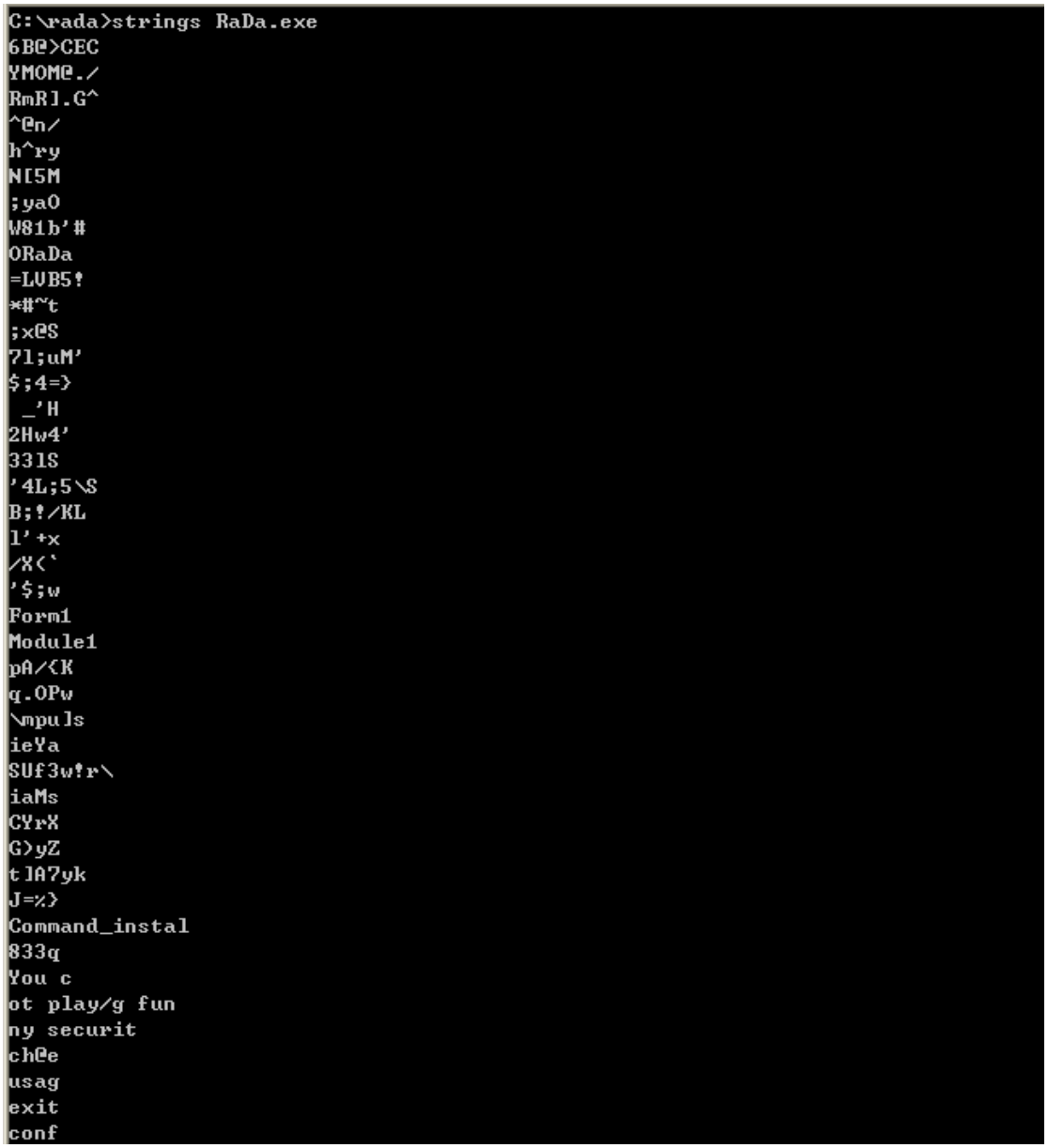
```
C:\rada>ls
RaDa.exe

C:\rada>file RaDa.exe
RaDa.exe: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
```

看到 RaDa.exe 是一个 Windows PE 可执行文件，并且有图形化窗口

2. 使用 PEiD 工具查看 RaDa.exe 的基本信息

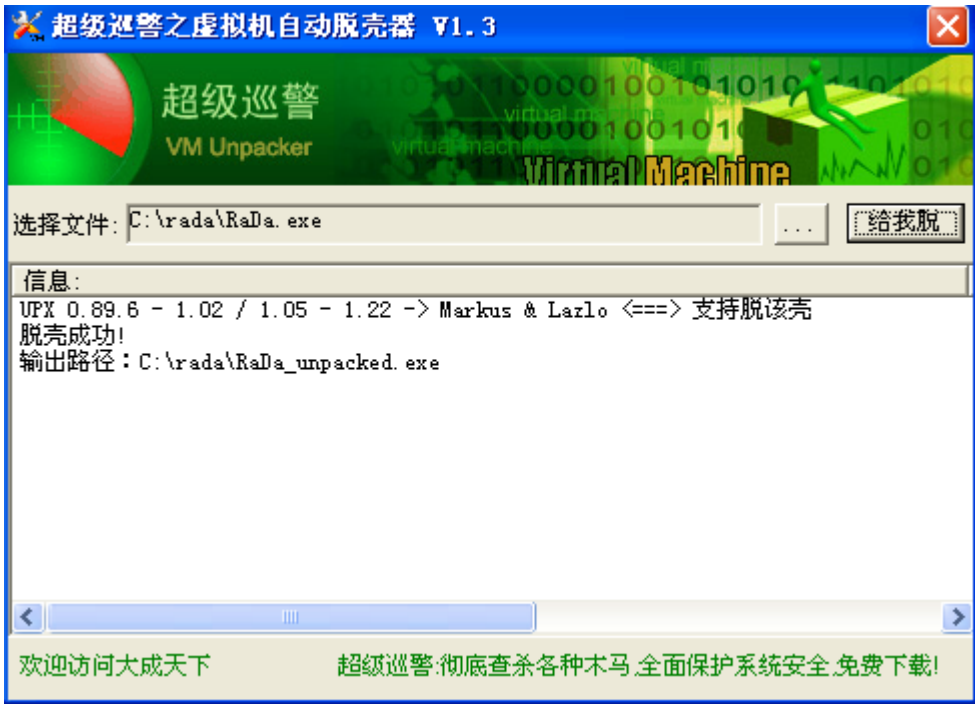
这里可以看到文件的入口点、偏移、文件类型、EP 短、汇编程序以及加壳类型

3. 使用 strings 命令查看 RaDa.exe 中可打印字符串



出现乱码的原因是因为文件被加壳，正常字符无法显示

4. 对 RaDa.exe 进行脱壳



尽管是经过修改的 UPX 壳，但是该自动化脱壳工具显然有这个壳的样本库，能够自动脱壳，省去了手工脱壳的麻烦

5. 再用 strings 查看脱壳后的 RaDa.exe(RaDa_unpacked.exe)

脱壳之后出现正常的字符串，再从中寻找有用信息