

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](http://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

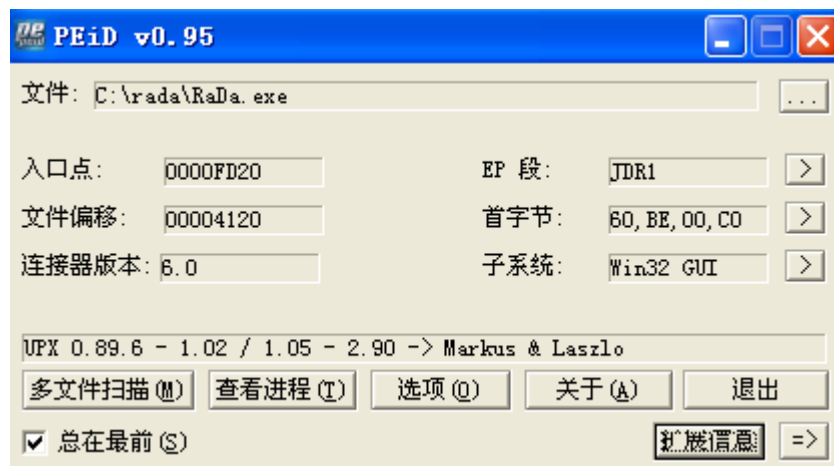
1. 使用 file 命令查看 RaDa.exe 的文件类型

```
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

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

```
6B@>CEC
```

```
YMOM@./
```

```
RmRl.G^
```

```
^@n/
```

```
h^ry
```

```
NI5M
```

```
;ya0
```

```
W81b'#
```

```
ORaDa
```

```
=LUB5!
```

```
*#^t
```

```
;x@S
```

```
71;uM'
```

```
$;4=>
```

```
_ 'H
```

```
2Hw4'
```

```
331S
```

```
'4L;5\S
```

```
B;!/KL
```

```
l' +x
```

```
/X<'
```

```
'$;w
```

```
Form1
```

```
Module1
```

```
pA/<K
```

```
q.OPw
```

```
\mpuls
```

```
ieYa
```

```
SUf3w!r\
```

```
iaMs
```

```
CYrX
```

```
G>yZ
```

```
t1A7yk
```

```
J=%>
```

```
Command_instal
```

```
833q
```

```
You c
```

```
ot play/g fun
```

```
ny securit
```

```
ch@e
```

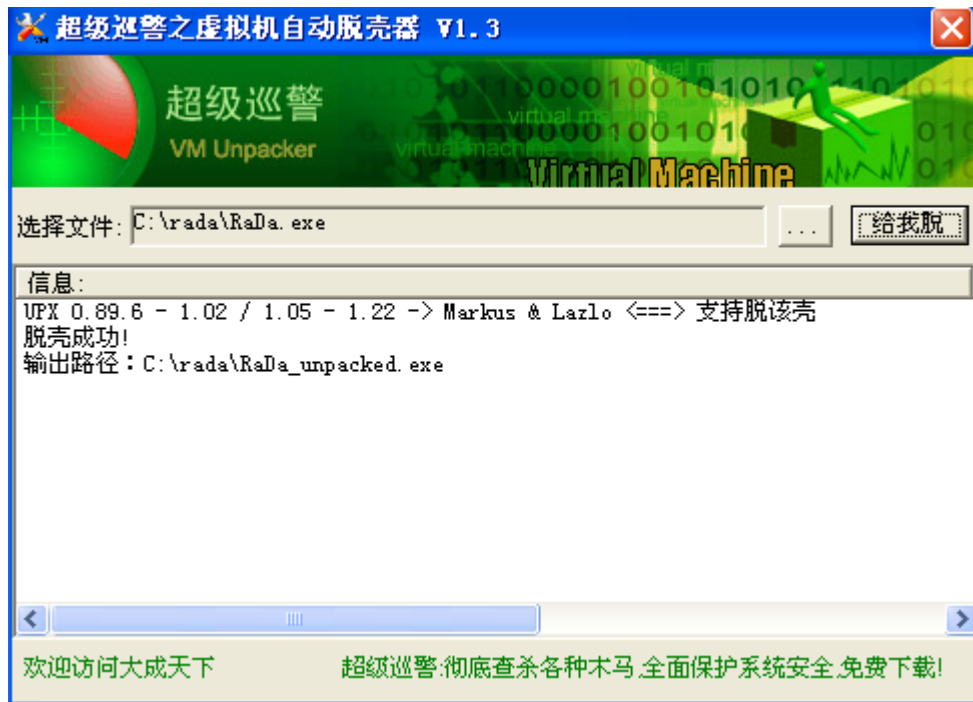
```
usag
```

```
exit
```

```
conf
```

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)

```
C:\rada>strings RaDa_unpacked.exe
_vbaVarTstGt
_vbaVarSub
_Clcos
_adj_fptan
_vbaVarMove
_vbaVarUargNofree
_vbaFreeVar
_vbaAryMove
_vbaStrUarMove
_vbaLenBstr
_vbaFreeVarList
_vbaVarIdiv
_vbaPut3
_vbaEnd
_adj_fdiv_m64
_vbaVarIndexStore
_vbaNextEachVar
_vbaFreeObjList
_vbaVarIndexLoadRef
_vbaStrErrUarCopy
_adj_fprem1
_vbaStrCat
_vbaSetSystemError
_vbaHresultCheckObj
_vbaLenUar
_adj_fdiv_m32
_vbaAryDestruct
_vbaLateMemSt
_vbaExitProc
_vbaVarForInit
_vbaOnError
_vbaObjSet
_adj_fdiv_m16i
_vbaObjSetAddrRef
_adj_fdivr_m16i
_vbaVarIndexLoad
_vbaBoolVarNull
_vbaUargVar
_vbaVarTstLt
_ClSin
_vbaVarZero
_vbaChkstk
```

脱壳之后出现正常的字符串，再从中寻找有用信息