软件安全－恶意代码机理与防护
3.7 资源节

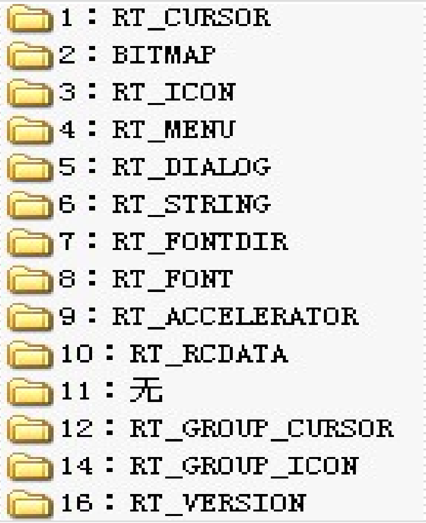
彭国军 教授

武汉大学国家网络安全学院

guojpeng@whu.edu.cn

3.7 资源节

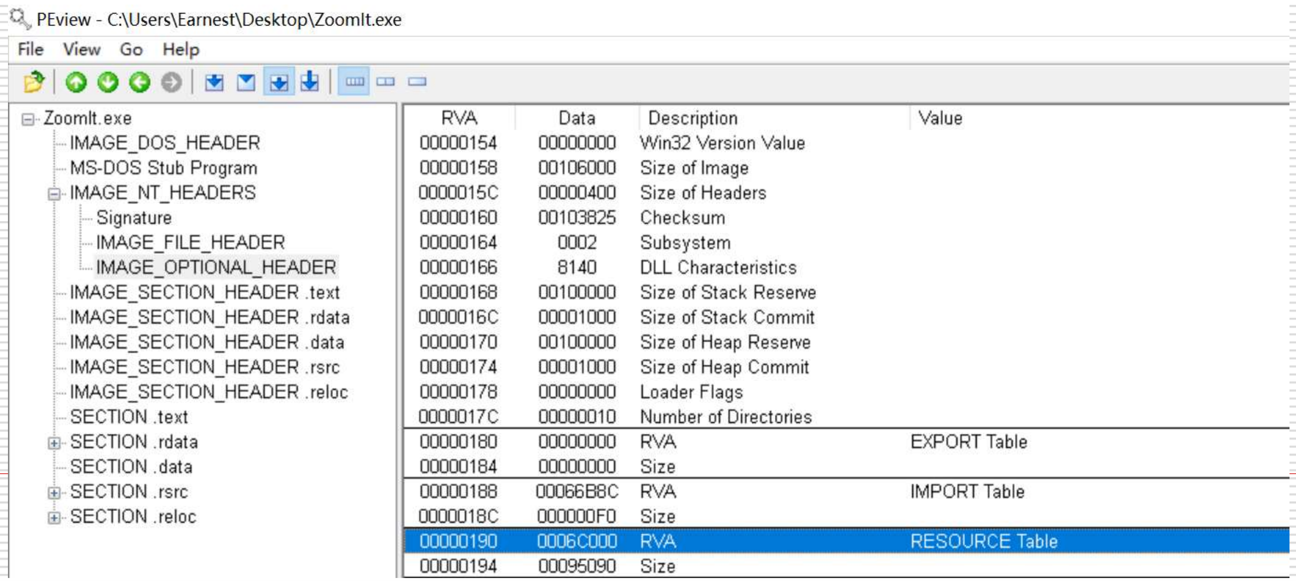
- 资源节一般名为.rsrc（resource）
- 这个节可存放程序需要用到的资源：
  - 如光标、位图、图标、菜单、对话框、字符串、字体目录、字体、加速键、光标组、图标组、版本等。



1：RT_CURSOR
2：BITMAP
3：RT_ICON
4：RT_MENU
5：RT_DIALOG
6：RT_STRING
7：RT_FONTDIR
8：RT_FONT
9：RT_ACCELERATOR
10：RT_RCDATA
11：无
12：RT_GROUP_CURSOR
14：RT_GROUP_ICON
16：RT_VERSION

1.如何定位资源目录位置?

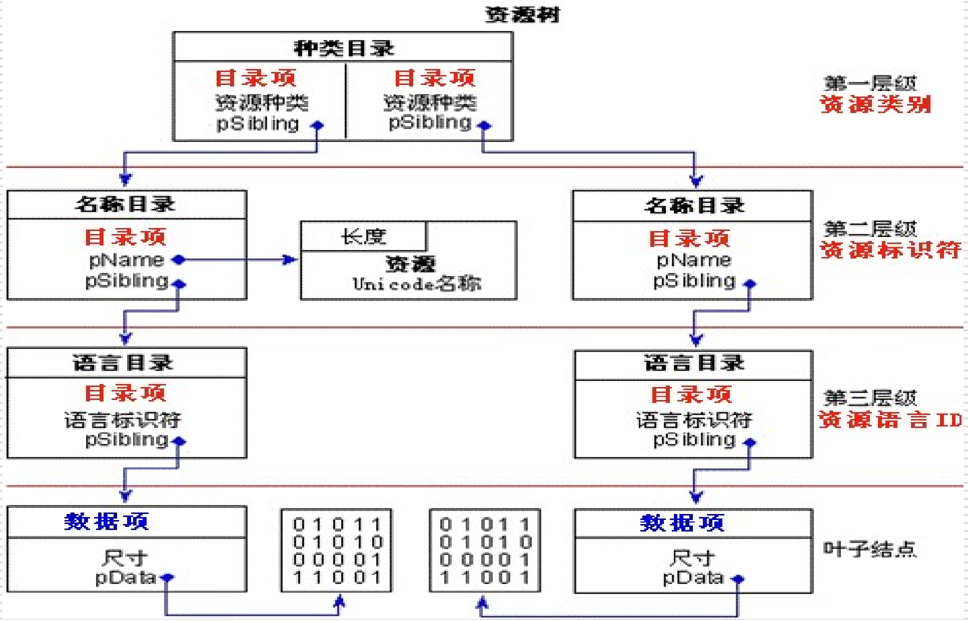
- 可选文件头的DataDirectory数组第3项。
  - 指向资源目录表开始位置（RVA）和大小。



```
ZoomIt.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
    Signature
    IMAGE_FILE_HEADER
    IMAGE_OPTIONAL_HEADER
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .rsrc
  SECTION .reloc
```

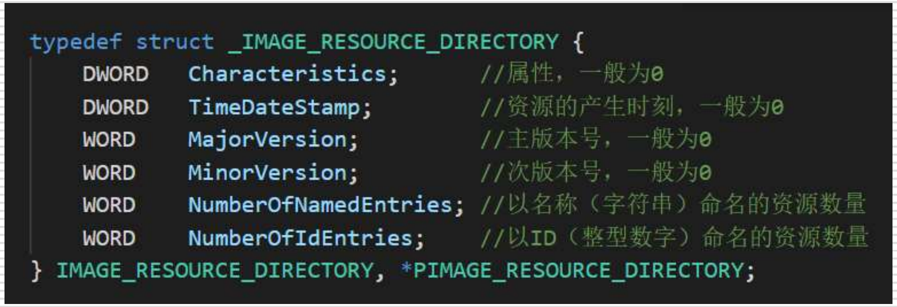
RVA	Data	Description	Value
00000154	00000000	Win32 Version Value	
00000158	00106000	Size of Image	
0000015C	00000400	Size of Headers	
00000160	00103825	Checksum	
00000164	0002	Subsystem	
00000166	8140	DLL Characteristics	
00000168	00100000	Size of Stack Reserve	
0000016C	00001000	Size of Stack Commit	
00000170	00100000	Size of Heap Reserve	
00000174	00001000	Size of Heap Commit	
00000178	00000000	Loader Flags	
0000017C	00000010	Number of Directories	
00000180	00000000	RVA	EXPORT Table
00000184	00000000	Size	
00000188	00066B8C	RVA	IMPORT Table
0000018C	000000F0	Size	
00000190	0006C000	RVA	RESOURCE Table
00000194	00095090	Size	

2.资源树的层次与结构

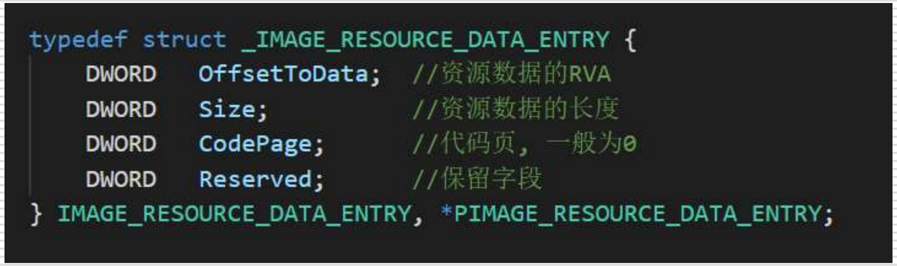


- □ 树的层次与类型
  - 资源类别、资源标识符、资源语言ID、数据
- □ 3个重要结构：
  - ■ 目录
    - IMAGE_RESOURCE_DIRECTORY
  - ■ 目录项
    - IMAGE_RESOURCE_DIRECTORY_ENTRY
  - ■ 数据项
    - IMAGE_RESOURCE_DATA_ENTRY

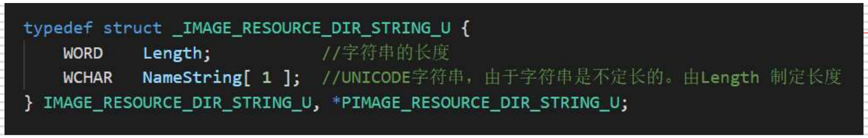
资源涉及到的数据结构



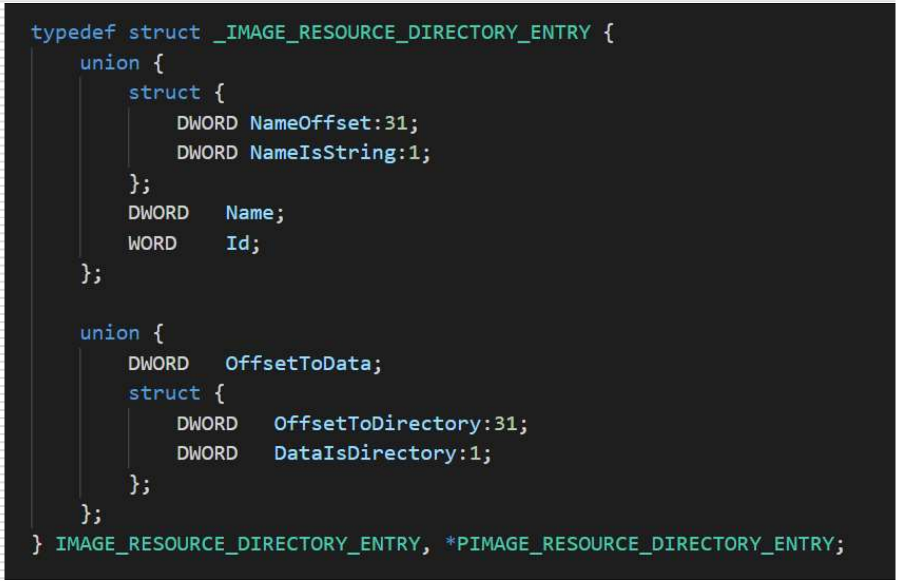
```
typedef struct _IMAGE_RESOURCE_DIRECTORY {
    DWORD   Characteristics;        //属性，一般为0
    DWORD   TimeDateStamp;          //资源的产生时刻，一般为0
    WORD    MajorVersion;           //主版本号，一般为0
    WORD    MinorVersion;           //次版本号，一般为0
    WORD    NumberOfNamedEntries; //以名称（字符串）命名的资源数量
    WORD    NumberOfIdEntries;      //以ID（整型数字）命名的资源数量
} IMAGE_RESOURCE_DIRECTORY, *PIMAGE_RESOURCE_DIRECTORY;
```



```
typedef struct _IMAGE_RESOURCE_DATA_ENTRY {
    DWORD   OffsetToData;   //资源数据的RVA
    DWORD   Size;           //资源数据的长度
    DWORD   CodePage;       //代码页，一般为0
    DWORD   Reserved;       //保留字段
} IMAGE_RESOURCE_DATA_ENTRY, *PIMAGE_RESOURCE_DATA_ENTRY;
```



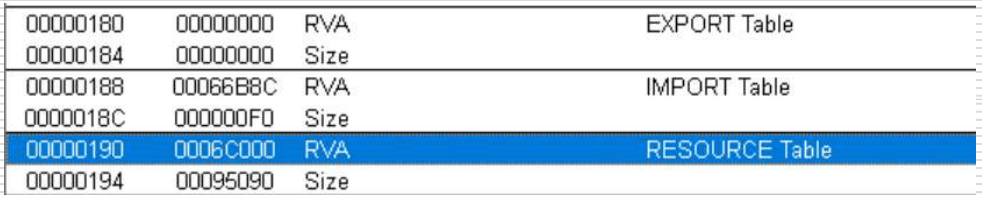
```
typedef struct _IMAGE_RESOURCE_DIR_STRING_U {
    WORD    Length;             //字符串的长度
    WCHAR   NameString[ 1 ];  //UNICODE字符串，由于字符串是不定长的。由Length 制定长度
} IMAGE_RESOURCE_DIR_STRING_U, *PIMAGE_RESOURCE_DIR_STRING_U;
```



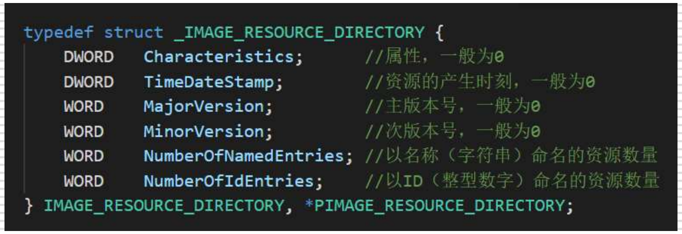
```
typedef struct _IMAGE_RESOURCE_DIRECTORY_ENTRY {
    union {
        struct {
            DWORD NameOffset:31;
            DWORD NameIsString:1;
        };
        DWORD   Name;
        WORD    Id;
    };

    union {
        DWORD   OffsetToData;
        struct {
            DWORD   OffsetToDirectory:31;
            DWORD   DataIsDirectory:1;
        };
    };
} IMAGE_RESOURCE_DIRECTORY_ENTRY, *PIMAGE_RESOURCE_DIRECTORY_ENTRY;
```

目录结构
IMAGE_RESOURCE_DIRECTORY

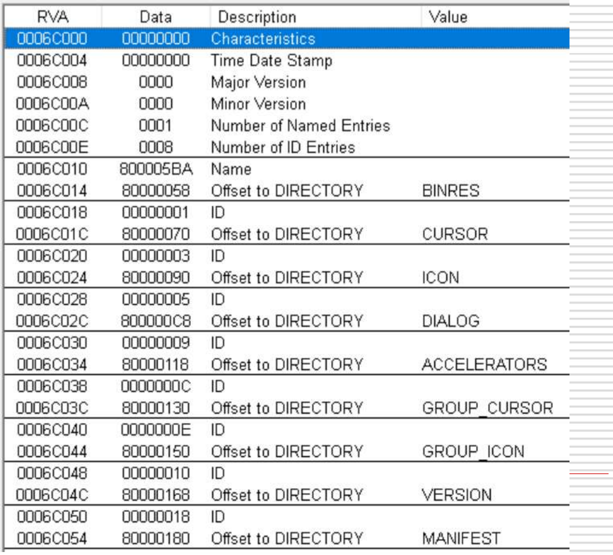
顺序	名字	大小 （字节）	描述
1	Characteritics	4	通常为0
2	TimeDateStamp	4	资源生成时间
3	MajorVersion	2	主版本号
4	MinorVersion	2	次版本号
5	NumberOfNamedEntries	2	以名字标识的资源数
6	NumberOfldEntries	2	以ID标识的资源数



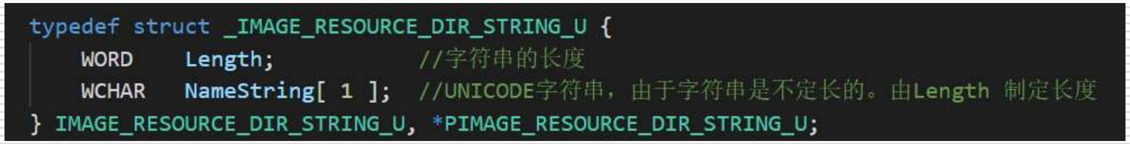
```
00000180   00000000   RVA                      EXPORT Table
00000184   00000000   Size
00000188   00066B8C   RVA                      IMPORT Table
0000018C   000000F0   Size
00000190   0006C000   RVA                      RESOURCE Table
00000194   00095090   Size
```



```
typedef struct _IMAGE_RESOURCE_DIRECTORY {
    DWORD   Characteristics;        //属性，一般为0
    DWORD   TimeDateStamp;          //资源的产生时刻，一般为0
    WORD    MajorVersion;           //主版本号，一般为0
    WORD    MinorVersion;           //次版本号，一般为0
    WORD    NumberOfNamedEntries; //以名称（字符串）命名的资源数量
    WORD    NumberOfIdEntries;      //以ID（整型数字）命名的资源数量
} IMAGE_RESOURCE_DIRECTORY, *PIMAGE_RESOURCE_DIRECTORY;
```

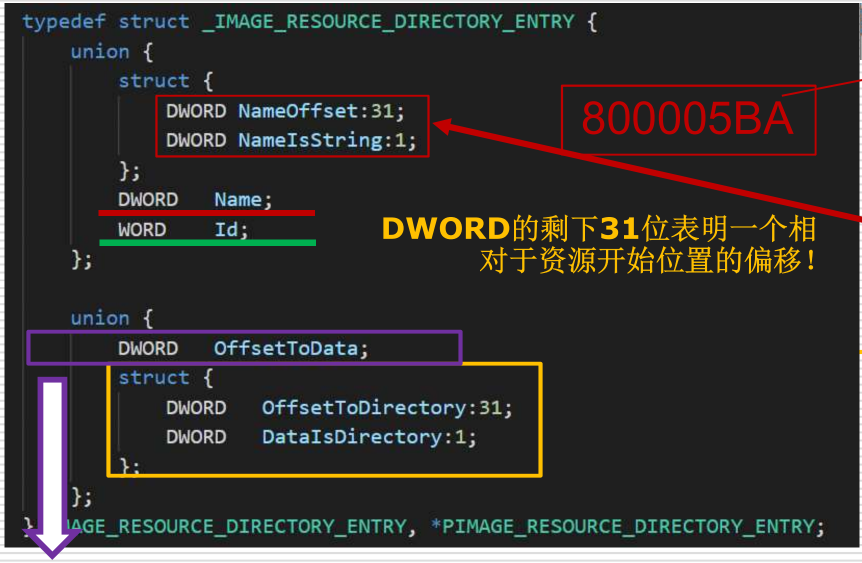


RVA	Data	Description	Value
0006C000	00000000	Characteristics	
0006C004	00000000	Time Date Stamp	
0006C008	0000	Major Version	
0006C00A	0000	Minor Version	
0006C00C	0001	Number of Named Entries	
0006C00E	0008	Number of ID Entries	
0006C010	800005BA	Name	
0006C014	80000058	Offset to DIRECTORY	BINRES
0006C018	00000001	ID	
0006C01C	80000070	Offset to DIRECTORY	CURSOR
0006C020	00000003	ID	
0006C024	80000090	Offset to DIRECTORY	ICON
0006C028	00000005	ID	
0006C02C	800000C8	Offset to DIRECTORY	DIALOG
0006C030	00000009	ID	
0006C034	80000118	Offset to DIRECTORY	ACCELERATORS
0006C038	0000000C	ID	
0006C03C	80000130	Offset to DIRECTORY	GROUP_CURSOR
0006C040	0000000E	ID	
0006C044	80000150	Offset to DIRECTORY	GROUP_ICON
0006C048	00000010	ID	
0006C04C	80000168	Offset to DIRECTORY	VERSION
0006C050	00000018	ID	
0006C054	80000180	Offset to DIRECTORY	MANIFEST



```
typedef struct _IMAGE_RESOURCE_DIR_STRING_U {
    WORD    Length;             //字符串的长度
    WCHAR   NameString[ 1 ];    //UNICODE字符串，由于字符串是不定长的。由Length 制定长度
} IMAGE_RESOURCE_DIR_STRING_U, *PIMAGE_RESOURCE_DIR_STRING_U;
```

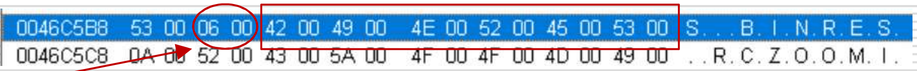
目录项结构
IMAGE_RESOURCE_DIRECTORY_ENTRY



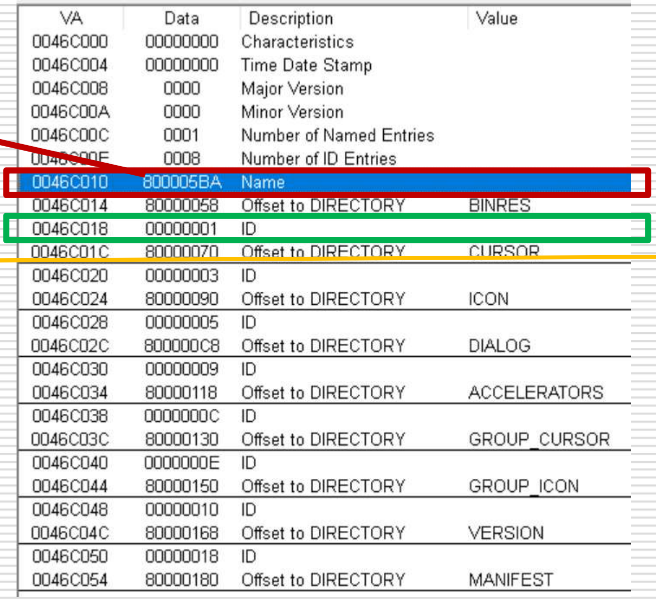
```
typedef struct _IMAGE_RESOURCE_DIRECTORY_ENTRY {
    union {
        struct {
            DWORD NameOffset:31;
            DWORD NameIsString:1;
        };
        DWORD   Name;
        WORD    Id;
    };

    union {
        DWORD   OffsetToData;
        struct {
            DWORD   OffsetToDirectory:31;
            DWORD   DataIsDirectory:1;
        };
    };
} IMAGE_RESOURCE_DIRECTORY_ENTRY, *PIMAGE_RESOURCE_DIRECTORY_ENTRY;
```

800005BA

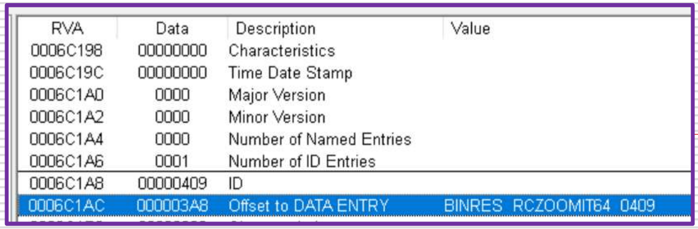
DWORD的剩下**31**位表明一个相对于资源开始位置的偏移！



```
0046C5B8  53 00 06 00 42 00 49 00  4E 00 52 00 45 00 53 00  S. . . B. I. N. R. E. S.
0046C5C8  0A 00 52 00 43 00 5A 00  4F 00 4F 00 4D 00 49 00  . . R. C. Z. O. O. M. I.
```



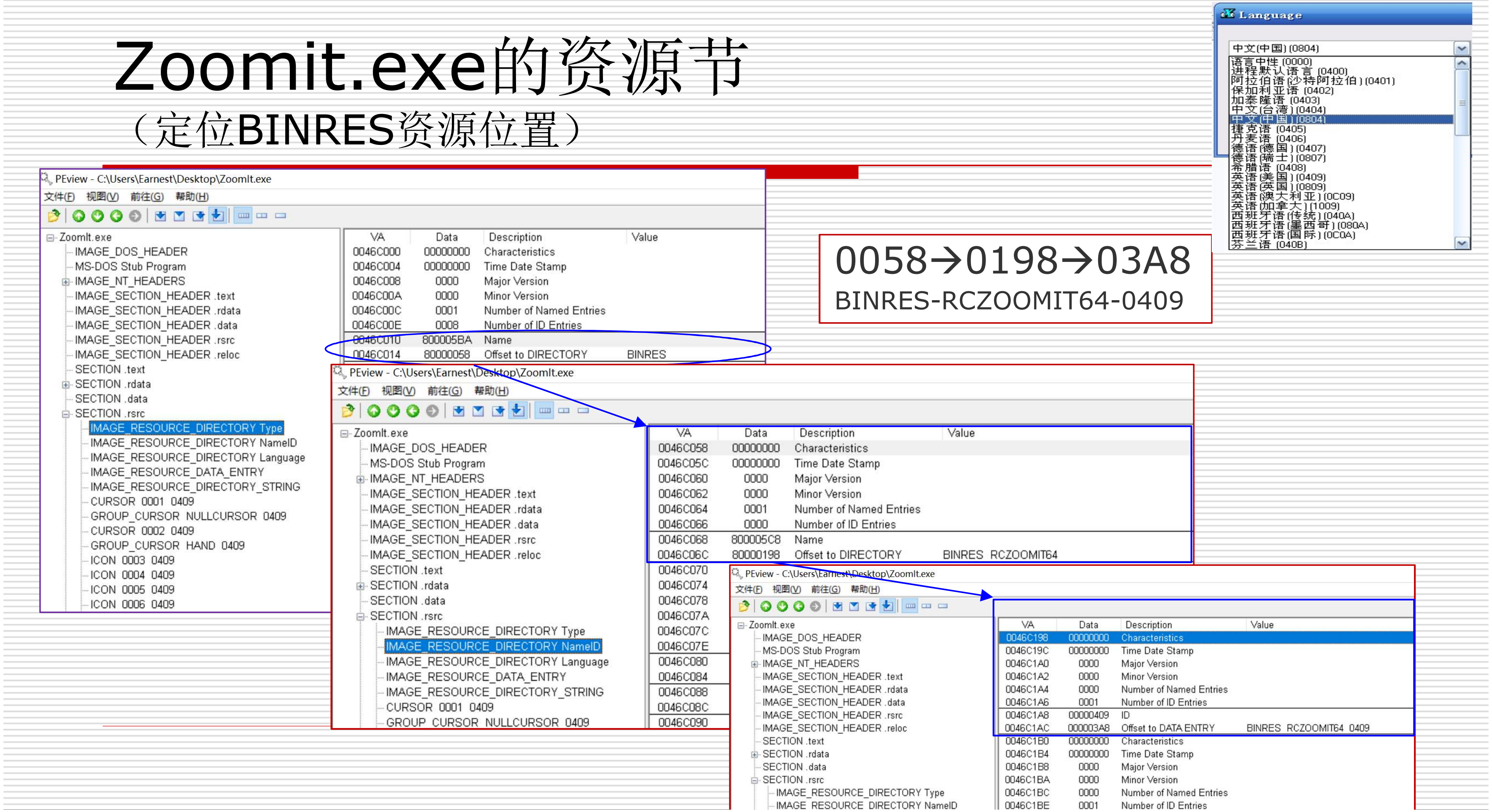
VA	Data	Description	Value
0046C000	00000000	Characteristics	
0046C004	00000000	Time Date Stamp	
0046C008	0000	Major Version	
0046C00A	0000	Minor Version	
0046C00C	0001	Number of Named Entries	
0046C00E	0008	Number of ID Entries	
0046C010	800005BA	Name	
0046C014	80000058	Offset to DIRECTORY	BINRES
0046C018	00000001	ID	
0046C01C	80000070	Offset to DIRECTORY	CURSOR
0046C020	00000003	ID	
0046C024	80000090	Offset to DIRECTORY	ICON
0046C028	00000005	ID	
0046C02C	800000C8	Offset to DIRECTORY	DIALOG
0046C030	00000009	ID	
0046C034	80000118	Offset to DIRECTORY	ACCELERATORS
0046C038	0000000C	ID	
0046C03C	80000130	Offset to DIRECTORY	GROUP_CURSOR
0046C040	0000000E	ID	
0046C044	80000150	Offset to DIRECTORY	GROUP_ICON
0046C048	00000010	ID	
0046C04C	80000168	Offset to DIRECTORY	VERSION
0046C050	00000018	ID	
0046C054	80000180	Offset to DIRECTORY	MANIFEST



RVA	Data	Description	Value
0006C198	00000000	Characteristics	
0006C19C	00000000	Time Date Stamp	
0006C1A0	0000	Major Version	
0006C1A2	0000	Minor Version	
0006C1A4	0000	Number of Named Entries	
0006C1A6	0001	Number of ID Entries	
0006C1A8	00000409	ID	
0006C1AC	000003A8	Offset to DATA ENTRY	BINRES RCZOOMIT64 0409

Zoomit.exe的资源节

（定位BINRES资源位置）



0058→0198→03A8

BINRES-RCZOOMIT64-0409

Language

中文(中国) (0804)

```
语言中性 (0000)
进程默认语言 (0400)
阿拉伯语(沙特阿拉伯) (0401)
保加利亚语 (0402)
加泰隆语 (0403)
中文(台湾) (0404)
中文(中国) (0804)
捷克语 (0405)
丹麦语 (0406)
德语(德国) (0407)
德语(瑞士) (0807)
希腊语 (0408)
英语(美国) (0409)
英语(英国) (0809)
英语(澳大利亚) (0C09)
英语(加拿大) (1009)
西班牙语(传统) (040A)
西班牙语(墨西哥) (080A)
西班牙语(国际) (0C0A)
芬兰语 (040B)
```

PEview - C:\Users\Earnest\Desktop\Zoomlt.exe

```
Zoomlt.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .rsrc
    IMAGE_RESOURCE_DIRECTORY Type
    IMAGE_RESOURCE_DIRECTORY NameID
    IMAGE_RESOURCE_DIRECTORY Language
    IMAGE_RESOURCE_DATA_ENTRY
    IMAGE_RESOURCE_DIRECTORY_STRING
    CURSOR 0001 0409
    GROUP_CURSOR NULLCURSOR 0409
    CURSOR 0002 0409
    GROUP_CURSOR HAND 0409
    ICON 0003 0409
    ICON 0004 0409
    ICON 0005 0409
    ICON 0006 0409
```

VA	Data	Description	Value
0046C000	00000000	Characteristics	
0046C004	00000000	Time Date Stamp	
0046C008	0000	Major Version	
0046C00A	0000	Minor Version	
0046C00C	0001	Number of Named Entries	
0046C00E	0008	Number of ID Entries	
0046C010	800005BA	Name	
0046C014	80000058	Offset to DIRECTORY	BINRES

PEview - C:\Users\Earnest\Desktop\Zoomlt.exe

```
Zoomlt.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .rsrc
    IMAGE_RESOURCE_DIRECTORY Type
    IMAGE_RESOURCE_DIRECTORY NameID
    IMAGE_RESOURCE_DIRECTORY Language
    IMAGE_RESOURCE_DATA_ENTRY
    IMAGE_RESOURCE_DIRECTORY_STRING
    CURSOR 0001 0409
    GROUP_CURSOR NULLCURSOR 0409
```

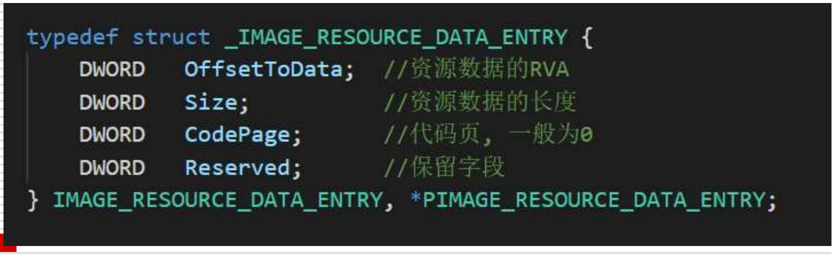
VA	Data	Description	Value
0046C058	00000000	Characteristics	
0046C05C	00000000	Time Date Stamp	
0046C060	0000	Major Version	
0046C062	0000	Minor Version	
0046C064	0001	Number of Named Entries	
0046C066	0000	Number of ID Entries	
0046C068	800005C8	Name	
0046C06C	80000198	Offset to DIRECTORY	BINRES RCZOOMIT64
0046C070			
0046C074			
0046C078			
0046C07A			
0046C07C			
0046C07E			
0046C080			
0046C084			
0046C088			
0046C08C			
0046C090			

PEview - C:\Users\Earnest\Desktop\Zoomlt.exe

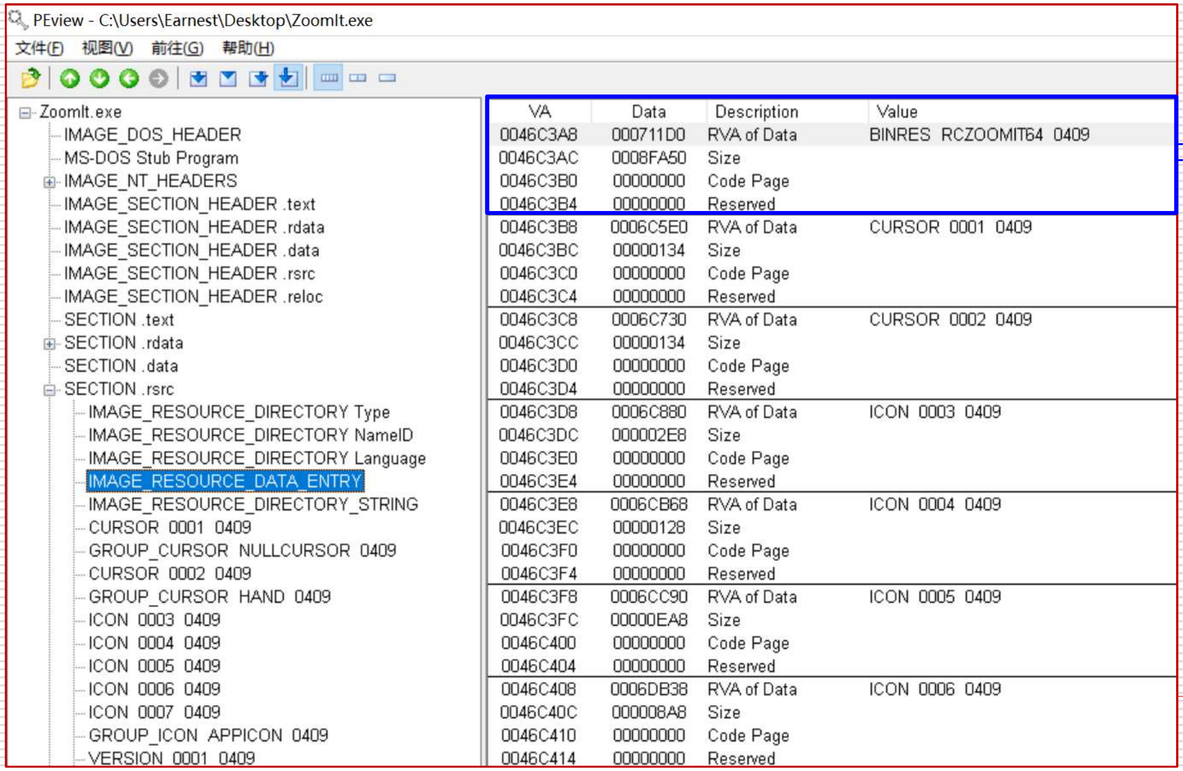
```
Zoomlt.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .rsrc
    IMAGE_RESOURCE_DIRECTORY Type
    IMAGE_RESOURCE_DIRECTORY NameID
```

VA	Data	Description	Value
0046C198	00000000	Characteristics	
0046C19C	00000000	Time Date Stamp	
0046C1A0	0000	Major Version	
0046C1A2	0000	Minor Version	
0046C1A4	0000	Number of Named Entries	
0046C1A6	0001	Number of ID Entries	
0046C1A8	00000409	ID	
0046C1AC	000003A8	Offset to DATA ENTRY	BINRES RCZOOMIT64 0409
0046C1B0	00000000	Characteristics	
0046C1B4	00000000	Time Date Stamp	
0046C1B8	0000	Major Version	
0046C1BA	0000	Minor Version	
0046C1BC	0000	Number of Named Entries	
0046C1BE	0001	Number of ID Entries	

Zoomit.exe的资源节
定位BINRES资源数据位置



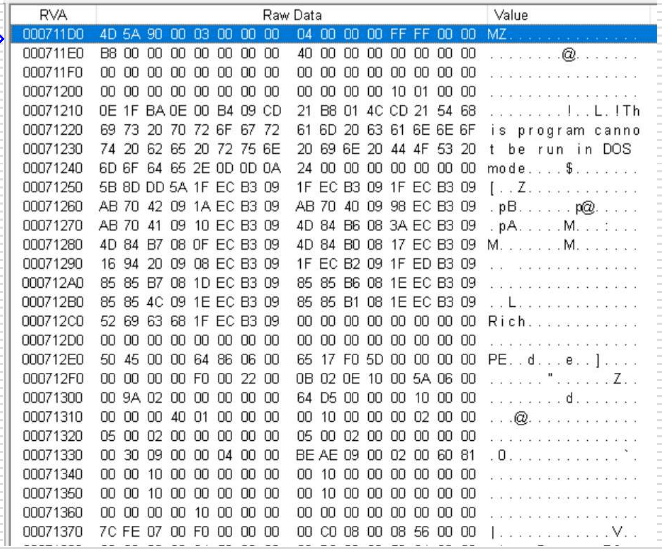
```
typedef struct _IMAGE_RESOURCE_DATA_ENTRY {
    DWORD   OffsetToData;   //资源数据的RVA
    DWORD   Size;           //资源数据的长度
    DWORD   CodePage;       //代码页，一般为0
    DWORD   Reserved;       //保留字段
} IMAGE_RESOURCE_DATA_ENTRY, *PIMAGE_RESOURCE_DATA_ENTRY;
```



PEview - C:\Users\Earnest\Desktop\ZoomIt.exe
文件(F) 视图(V) 前往(G) 帮助(H)

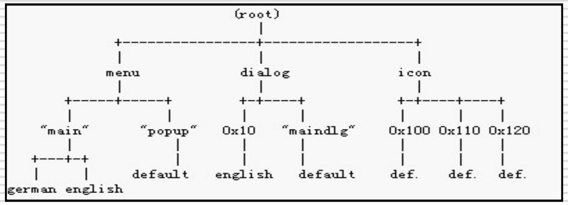
- ZoomIt.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .rdata
  - IMAGE_SECTION_HEADER .data
  - IMAGE_SECTION_HEADER .rsrc
  - IMAGE_SECTION_HEADER .reloc
  - SECTION .text
  - SECTION .rdata
  - SECTION .data
  - SECTION .rsrc
    - IMAGE_RESOURCE_DIRECTORY Type
    - IMAGE_RESOURCE_DIRECTORY NameID
    - IMAGE_RESOURCE_DIRECTORY Language
    - IMAGE_RESOURCE_DATA_ENTRY
    - IMAGE_RESOURCE_DIRECTORY_STRING
    - CURSOR 0001 0409
    - GROUP_CURSOR NULLCURSOR 0409
    - CURSOR 0002 0409
    - GROUP_CURSOR HAND 0409
    - ICON 0003 0409
    - ICON 0004 0409
    - ICON 0005 0409
    - ICON 0006 0409
    - ICON 0007 0409
    - GROUP_ICON APPICON 0409
    - VERSION 0001 0409

VA	Data	Description	Value
0046C3A8	000711D0	RVA of Data	BINRES RCZOOMIT64 0409
0046C3AC	0008FA50	Size	
0046C3B0	00000000	Code Page	
0046C3B4	00000000	Reserved	
0046C3B8	0006C5E0	RVA of Data	CURSOR 0001 0409
0046C3BC	00000134	Size	
0046C3C0	00000000	Code Page	
0046C3C4	00000000	Reserved	
0046C3C8	0006C730	RVA of Data	CURSOR 0002 0409
0046C3CC	00000134	Size	
0046C3D0	00000000	Code Page	
0046C3D4	00000000	Reserved	
0046C3D8	0006C880	RVA of Data	ICON 0003 0409
0046C3DC	000002E8	Size	
0046C3E0	00000000	Code Page	
0046C3E4	00000000	Reserved	
0046C3E8	0006CB68	RVA of Data	ICON 0004 0409
0046C3EC	00000128	Size	
0046C3F0	00000000	Code Page	
0046C3F4	00000000	Reserved	
0046C3F8	0006CC90	RVA of Data	ICON 0005 0409
0046C3FC	00000EA8	Size	
0046C400	00000000	Code Page	
0046C404	00000000	Reserved	
0046C408	0006DB38	RVA of Data	ICON 0006 0409
0046C40C	000008A8	Size	
0046C410	00000000	Code Page	
0046C414	00000000	Reserved	



```
RVA       Raw Data                                          Value
000711D0  4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ..............
000711E0  B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
000711F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00071200  00 00 00 00 00 00 00 00  00 00 00 00 10 01 00 00  ................
00071210  0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ........!..L.!Th
00071220  69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
00071230  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS 
00071240  6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode....$.......
00071250  5B 8D DD 5A 1F EC B3 09  1F EC B3 09 1F EC B3 09  [..Z............
00071260  AB 70 42 09 1A EC B3 09  AB 70 40 09 98 EC B3 09  .pB.....p@......
00071270  AB 70 41 09 10 EC B3 09  4D 84 B6 08 3A EC B3 09  .pA.....M...:...
00071280  4D 84 B7 08 0F EC B3 09  4D 84 B0 08 17 EC B3 09  M.......M.......
00071290  16 94 20 09 08 EC B3 09  1F EC B2 09 1F ED B3 09  ................
000712A0  85 85 B7 08 1D EC B3 09  85 85 B6 08 1E EC B3 09  ................
000712B0  85 85 4C 09 1E EC B3 09  85 85 B1 08 1E EC B3 09  ..L.............
000712C0  52 69 63 68 1F EC B3 09  00 00 00 00 00 00 00 00  Rich............
000712D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000712E0  50 45 00 00 64 86 06 00  65 17 F0 5D 00 00 00 00  PE..d...e..]....
000712F0  00 00 00 00 F0 00 22 00  0B 02 0E 10 00 5A 06 00  ......"......Z..
00071300  00 9A 02 00 00 00 00 00  64 D5 00 00 00 10 00 00  ........d.......
00071310  00 00 00 40 01 00 00 00  00 10 00 00 00 02 00 00  ...@............
00071320  05 00 02 00 00 00 00 00  05 00 02 00 00 00 00 00  ................
00071330  00 30 09 00 00 04 00 00  BE AE 09 00 02 00 60 81  .0............`.
00071340  00 00 10 00 00 00 00 00  00 10 00 00 00 00 00 00  ................
00071350  00 00 10 00 00 00 00 00  00 10 00 00 00 00 00 00  ................
00071360  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  ................
00071370  7C FE 07 00 F0 00 00 00  00 C0 08 00 08 56 00 00  |............V..
```

定位资源



- □ 资源一般使用树来保存，通常包含4层，最高层是类型，其次是名字，然后是语言，最后是具体资源数据描述。
- □ 定位方法：
  - ■ 通过DataDirectory第3项找到资源目录开始位置，根据目标资源类型遍历其目录项，定位到二级目录位置。
  - ■ 在第二级目录，根据目标资源名称遍历其目录项，定位为三级目录位置。
  - ■ 在第三级目录，根据目标资源语言遍历其目录项，定位资源数据项位置。
  - ■ 在第四级，到达资源数据项（IMAGE_RESOURCE_DATA_ENTRY），通过第1、2两项，找到资源数据的RVA和大小。

恶意代码的部分应用

- □ 攻击载荷存储与释放（如StuxNet）
- □ 目标程序的图标替换（感染，如熊猫烧香待解决的问题）
- □ 图标伪装（EXE文件更改为文件夹图标、pdf文档图标等）
- □ …