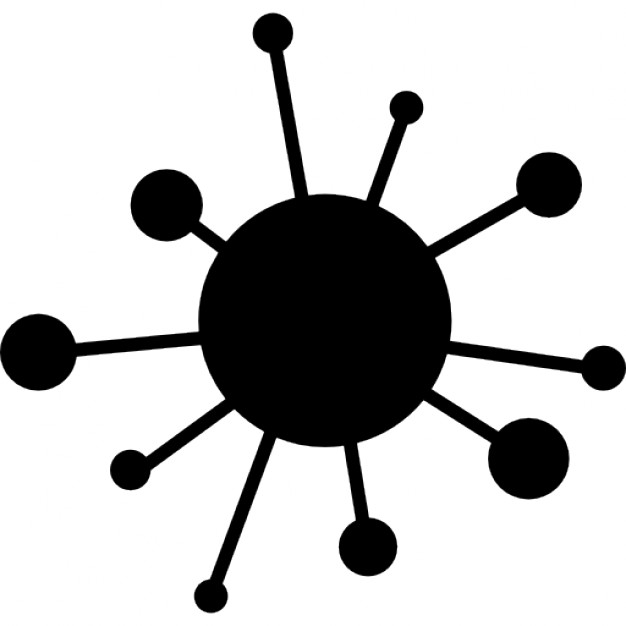
# 计算机病毒学

BMP图像还原



学号：0x091395

姓名：uknowho

还原步骤

1. 用WINHEX打开logonp.bp文件：

00000000 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 € € €€

00000010 80 00 00 00 80 00 80 00 80 80 00 00 C0 C0 C0 00 € € € €€ 览?

00000020 C0 DC C0 00 F0 CA A6 00 00 20 40 00 00 20 60 00 儡?鹗? @ `

00000030 00 20 80 00 00 20 A0 00 00 20 C0 00 00 20 E0 00 € ? ? ?

00000040 00 40 00 00 00 40 20 00 00 40 40 00 00 40 60 00 @ @ @@ @`

00000050 00 40 80 00 00 40 A0 00 00 40 C0 00 00 40 E0 00 @€ @? @? @?

00000060 00 60 00 00 00 60 20 00 00 60 40 00 00 60 60 00 ` ` `@ ``

00000070 00 60 80 00 00 60 A0 00 00 60 C0 00 00 60 E0 00 `€ `? `? `?

00000080 00 80 00 00 00 80 20 00 00 80 40 00 00 80 60 00 € € €@ €`

00000090 00 80 80 00 00 80 A0 00 00 80 C0 00 00 80 E0 00 €€ €? €? €?

000000A0 00 A0 00 00 00 A0 20 00 00 A0 40 00 00 A0 60 00 ? ? 燖 燻

000000B0 00 A0 80 00 00 A0 A0 00 00 A0 C0 00 00 A0 E0 00 爛 牋 犂 犩

000000C0 00 C0 00 00 00 C0 20 00 00 C0 40 00 00 C0 60 00 ? ? 繞 繾

000000D0 00 C0 80 00 00 C0 A0 00 00 C0 C0 00 00 C0 E0 00 纮 罓 览 类

000000E0 00 E0 00 00 00 E0 20 00 00 E0 40 00 00 E0 60 00 ? ? 郂 郹

1. 发现源文件缺少BMP文件头，和位图信息头。添加54字节数据到源文件头。WINHEX中步骤：
2. 编辑🡪粘贴0字节
3. 输入字节数54
4. 复制正常BMP位图文件头(54字节)到logonp.bm新添加的54字节处。WINHEX步骤：
5. 选中正常文件头，右键🡪编辑🡪复制选快🡪正常
6. 光标置于logonp.bm文件头处，右键🡪编辑🡪剪贴板数据🡪写入
7. 修改相应文件头数据。具体步骤参见附录1。
8. 修改后缀名为.bmp

附录1 logonp.bm文件头数据修改步骤：

对照附录2 BMP图像头部数据结构进行修改。

1. 整个BMP文件大小应为481,078字节，16进制为：00075736。
2. 修改文件宽度为：00000320高度为：00000258（800\*600）
3. 图像位数改为08（8位）
4. 修改后文件头数据如下：

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F

00000000 42 4D 36 57 07 00 00 00 00 00 36 04 00 00 28 00 BM6W 6 (

00000010 00 00 20 03 00 00 58 02 00 00 01 00 08 00 00 00 X

00000020 00 00 00 00 00 00 C4 0E 00 00 C4 0E 00 00 00 01 ? ?

00000030 00 00 00 01 00 00

1. 部分还原图数据:

00000000 42 4D 36 57 07 00 00 00 00 00 36 04 00 00 28 00 BM6W 6 (

00000010 00 00 20 03 00 00 58 02 00 00 01 00 08 00 00 00 X

00000020 00 00 00 00 00 00 C4 0E 00 00 C4 0E 00 00 00 01 ? ?

00000030 00 00 00 01 00 00 00 00 00 FF 00 00 80 FF 00 80  € €

00000040 00 FF 00 80 80 FF 80 00 00 FF 80 00 80 FF 80 80  €€€ € €€€

00000050 00 FF C0 C0 C0 FF C0 DC C0 FF F0 CA A6 FF 00 20 览?儡?鹗?

00000060 40 FF 00 20 60 FF 00 20 80 FF 00 20 A0 FF 00 20 @ ` € ?

00000070 C0 FF 00 20 E0 FF 00 40 00 FF 00 40 20 FF 00 40 ? ? @  @  @

00000080 40 FF 00 40 60 FF 00 40 80 FF 00 40 A0 FF 00 40 @ @` @€ @? @

00000090 C0 FF 00 40 E0 FF 00 60 00 FF 00 60 20 FF 00 60 ? @? `  `  `

000000A0 40 FF 00 60 60 FF 00 60 80 FF 00 60 A0 FF 00 60 @ `` `€ `? `

000000B0 C0 FF 00 60 E0 FF 00 80 00 FF 00 80 20 FF 00 80 ? `? €  €  €

000000C0 40 FF 00 80 60 FF 00 80 80 FF 00 80 A0 FF 00 80 @ €` €€ €? €

000000D0 C0 FF 00 80 E0 FF 00 A0 00 FF 00 A0 20 FF 00 A0 ? €? ? ? ?

000000E0 40 FF 00 A0 60 FF 00 A0 80 FF 00 A0 A0 FF 00 A0 @ 燻 爛 牋 ?

000000F0 C0 FF 00 A0 E0 FF 00 C0 00 FF 00 C0 20 FF 00 C0 ? 犩 ? ? ?

00000100 40 FF 00 C0 60 FF 00 C0 80 FF 00 C0 A0 FF 00 C0 @ 繾 纮 罓 ?

00000110 C0 FF 00 C0 E0 FF 00 E0 00 FF 00 E0 20 FF 00 E0 ? 类 ? ? ?

00000120 40 FF 00 E0 60 FF 00 E0 80 FF 00 E0 A0 FF 00 E0 @ 郹 鄝 酄 ?

00000130 C0 FF 00 E0 E0 FF 40 00 00 FF 40 00 20 FF 40 00 ? 噜@ @ @

00000140 40 FF 40 00 60 FF 40 00 80 FF 40 00 A0 FF 40 00 @@ `@ €@ ?@

00000150 C0 FF 40 00 E0 FF 40 20 00 FF 40 20 20 FF 40 20 ?@ ?@ @ @

00000160 40 FF 40 20 60 FF 40 20 80 FF 40 20 A0 FF 40 20 @@ `@ €@ ?@

00000170 C0 FF 40 20 E0 FF 40 40 00 FF 40 40 20 FF 40 40 ?@ ?@@ @@ @@

00000180 40 FF 40 40 60 FF 40 40 80 FF 40 40 A0 FF 40 40 @@@`@@€@@?@@

00000190 C0 FF 40 40 E0 FF 40 60 00 FF 40 60 20 FF 40 60 ?@@?@` @` @`

000001A0 40 FF 40 60 60 FF 40 60 80 FF 40 60 A0 FF 40 60 @@``@`€@`?@`

000001B0 C0 FF 40 60 E0 FF 40 80 00 FF 40 80 20 FF 40 80 ?@`?@€ @€ @€

000001C0 40 FF 40 80 60 FF 40 80 80 FF 40 80 A0 FF 40 80 @@€`@€€@€?@€

000001D0 C0 FF 40 80 E0 FF 40 A0 00 FF 40 A0 20 FF 40 A0 ?@€?@?@?@?

000001E0 40 FF 40 A0 60 FF 40 A0 80 FF 40 A0 A0 FF 40 A0 @@燻@爛@牋@?

000001F0 C0 FF 40 A0 E0 FF 40 C0 00 FF 40 C0 20 FF 40 C0 ?@犩@?@?@?



图1 还原图

附录2 BMP图像头

BMP图像组成如表1：

表1：BMP文件组织形式

|  |  |  |
| --- | --- | --- |
| 数据段名称 | 对应结构体(WINDOWS) | 大小（字节） |
| BMP文件头 | BITMAPFILEHEADER | 14 |
| 位图文件信息头 | BMP\_INFOHEADER | 40 |
| 调色板 | --- | --- |
| 位图数据 | --- | --- |

位图文件头(bmp file header)：提供文件的格式、大小等信息

typedef struct tagBITMAPFILEHEADER

{

UINT16 bfType; //2Bytes，424D必须为“BM”

DWORD bfSize; //4Bytes，整个BMP文件的大小

UINT16 bfReserved1; //2Bytes，保留，为0

UINT16 bfReserved2; //2Bytes，保留，为0

DWORD bfOffBits; //4Bytes，文件起始位置到图像像素数据的字节偏移量

}BITMAPFILEHEADER;

◆位图信息头(bitmap information)：提供图像数据的尺寸、位平面数、压缩方式、颜色索引等信息

typedef struct \_tagBMP\_INFOHEADER

{

DWORD biSize; //4Bytes，INFOHEADER结构体大小

LONG biWidth; //4Bytes，图像宽度（以像素为单位）

LONG biHeight; //4Bytes，图像高度

WORD biPlanes; //2Bytes，图像数据平面，BMP存储RGB数据，因此总为1

WORD biBitCount; //2Bytes，图像像素位数

DWORD biCompression; //4Bytes， 0：不压缩，1：RLE8，2：RLE4

DWORD biSizeImage; //4Bytes， 4字节对齐的图像数据大小

LONG biXPelsPerMeter; //4 Bytes，用象素/米表示的水平分辨率

LONG biYPelsPerMeter; //4 Bytes，用象素/米表示的垂直分辨率

DWORD biClrUsed; //4 Bytes，实际使用的调色板索引数，0：使用所有的调色板索引

DWORD biClrImportant; //4 Bytes，重要的调色板索引数,0：所有的调色板索引都重要

}BMP\_INFOHEADER;