CTF-伪加密

原创

RyanWang0000 于 2019-10-21 12:17:35 发布 1662 收藏 12

分类专栏： CTF-crypt 文章标签： CTF crypto

本文链接：https://blog.csdn.net/qq_32350719/article/details/102661596

伪加密

题目来源：buuCTF-crypto-zip伪加密

原理

zip伪加密是在文件头的加密标志位做修改，进而再打开文件时识被别为加密压缩包。

背景

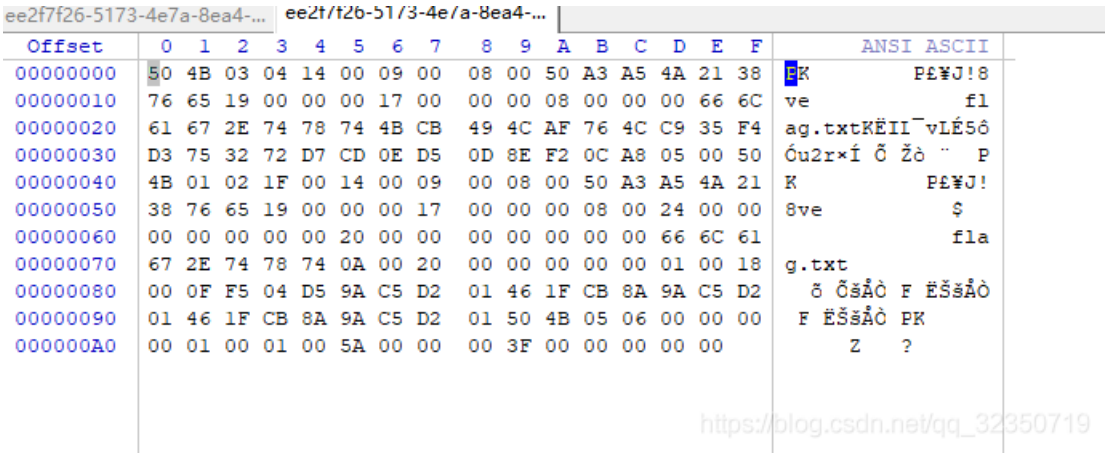
一个 ZIP 文件由三个部分组成：

压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志

详情：http://blog.csdn.net/wclxyn/article/details/7288994

实例

用Winhex工具打开zip文件查看其十六进制编码，图如下：



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	50	4B	03	04	14	00	09	00	08	00	50	A3	A5	4A	21	38	PK P£¥J!8
00000010	76	65	19	00	00	00	17	00	00	00	08	00	00	00	66	6C	ve fl
00000020	61	67	2E	74	78	74	4B	CB	49	4C	AF	76	4C	C9	35	F4	ag.txtKËIL¯vLÉ5ô
00000030	D3	75	32	72	D7	CD	0E	D5	0D	8E	F2	0C	A8	05	00	50	Óu2r×Í Õ Žò ¨ P
00000040	4B	01	02	1F	00	14	00	09	00	08	00	50	A3	A5	4A	21	K P£¥J!
00000050	38	76	65	19	00	00	00	17	00	00	00	08	00	24	00	00	8ve $
00000060	00	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61	fla
00000070	67	2E	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	g.txt
00000080	00	0F	F5	04	D5	9A	C5	D2	01	46	1F	CB	8A	9A	C5	D2	õ ÕšÅÒ F ËŠšÅÒ
00000090	01	46	1F	CB	8A	9A	C5	D2	01	50	4B	05	06	00	00	00	F ËŠšÅÒ PK
000000A0	00	01	00	01	00	5A	00	00	00	3F	00	00	00	00	00		Z ?

a.压缩源文件数据区：

50 4B 03 04：这是头文件标记（0x04034b50）
14 00：解压文件所需 pkware 版本
09 00：全局方式位标记（有无加密）
08 00：压缩方式
50 A3：最后修改文件时间
A5 4A：最后修改文件日期
21 38 76 64：CRC-32校验（1480B516）
19 00 00 00：压缩后尺寸（25）
17 00 00 00：未压缩尺寸（23）
08 00：文件名长度
00 00：扩展记录长度

666C61672E7478744BCB494CAF764CC935F4D3753272D7CD0ED50D8EF20CA80500

b.压缩源文件目录区：

50 4B 01 02：目录中文件文件头标记(0x02014b50)
1F 00：压缩使用的 pkware 版本
14 00：解压文件所需 pkware 版本
09 00：全局方式位标记（有无加密，这个更改这里进行伪加密，改为09 00打开就会提示有密码了）
08 00：压缩方式
50 A3：最后修改文件时间
A5 4A：最后修改文件日期
21 38 76 65：CRC-32校验（1480B516）
19 00 00 00：压缩后尺寸（25）
17 00 00 00：未压缩尺寸（23）
08 00：文件名长度
24 00：扩展字段长度
00 00：文件注释长度
00 00：磁盘开始号
00 00：内部文件属性
20 00 00 00：外部文件属性
00 00 00 00：局部头部偏移量
666C61672E7478740A00200000000000010018000FF504D59AC5D201461FCB8A9AC5D201461FCB8A9AC5D201

c.压缩源文件目录结束标志：

50 4B 05 06：目录结束标记
00 00：当前磁盘编号
00 00：目录区开始磁盘编号
01 00：本磁盘上纪录总数
01 00：目录区中纪录总数
5A 00 00 00：目录区尺寸大小
3F 00 00 00：目录区对第一张磁盘的偏移量
00 00 00：ZIP 文件注释长度

识别真假加密

无加密
压缩源文件数据区的全局加密应当为00 00
且压缩源文件目录区的全局方式位标记应当为00 00

假加密

压缩源文件数据区的全局加密应当为00 00
且压缩源文件目录区的全局方式位标记应当为09 00

真加密

压缩源文件数据区的全局加密应当为09 00
且压缩源文件目录区的全局方式位标记应当为09 00

把09 00 改成00 00 之后，保存，重新打开，即可看到flag