

PNG图片隐写IDAT分析（3）

原创

tdcoming 于 2018-08-20 19:23:12 发布 15879 收藏 25

分类专栏: [CTF](#) 文章标签: [PNG隐写 ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_29647709/article/details/81876374

版权



[CTF 专栏收录该内容](#)

12 篇文章 0 订阅

订阅专栏

使用工具pngcheck

命令: `pngcheck.exe -v sctf.png`

```
chunk IDAT at offset 0x10008, length 65524
zlib: deflated, 32K window, fast compression
chunk IDAT at offset 0x10008, length 65524
chunk IDAT at offset 0x20008, length 65524
chunk IDAT at offset 0x30008, length 65524
chunk IDAT at offset 0x40008, length 65524
chunk IDAT at offset 0x50008, length 65524
chunk IDAT at offset 0x60008, length 65524
chunk IDAT at offset 0x70008, length 65524
chunk IDAT at offset 0x80008, length 65524
chunk IDAT at offset 0x90008, length 65524
chunk IDAT at offset 0xa0008, length 65524
chunk IDAT at offset 0xb0008, length 65524
chunk IDAT at offset 0xc0008, length 65524
chunk IDAT at offset 0xd0008, length 65524
chunk IDAT at offset 0xe0008, length 65524
chunk IDAT at offset 0xf0008, length 65524
chunk IDAT at offset 0x100008, length 65524
chunk IDAT at offset 0x110008, length 65524
chunk IDAT at offset 0x120008, length 65524
chunk IDAT at offset 0x130008, length 65524
chunk IDAT at offset 0x140008, length 65524
chunk IDAT at offset 0x150008, length 45027
chunk IDAT at offset 0x15aff7, length 138
chunk IEND at offset 0x15b08d, length 0
No errors detected in sctf.png (28 chunks, 36.8% compression)
```

发现有个异常的IDAT 0X15aff7

```
0 95 00 FA 54 0D 21 BD BA 02 FF 3F 01 E7 98 5F 68 |.úT.!¼².ÿ?.ç|^h
0 95 8F CD 00 00 00 8A 49 44 41 54 78 9C 5D 91 01 |.í...IDAT[?]'.
0 12 80 40 08 02 BF 04 FF FF 5C 75 29 4B 55 37 73 |.l@..¿.ÿÿ\u)KU7s
0 8A 21 A2 7D 1E 49 CF D1 7D B3 93 7A 92 E7 E6 03 |lç}.IÎÑ}³lz'çæ.
0 88 0A 6D 48 51 00 90 1F B0 41 01 53 35 0D E8 31 |.mHQ...°A.S5.èl
0 12 EA 2D 51 C5 4C E2 E5 85 B1 5A 2F C7 8E 88 72 |.ê-QÁLáâ!±Z/Çllr
0 F5 1C 6F C1 88 18 82 F9 3D 37 2D EF 78 E6 65 B0 |ð.oÁ|.lù=7-ixæ°
0 C3 6C 52 96 22 A0 A4 55 88 13 88 33 A1 70 A2 07 |ÄlRl" *Ul.l3ipç.
0 1D DC D1 82 19 DB 8C 0D 46 5D 8B 69 89 71 96 45 |.ÜÑ|.Ü|.Fj|i|q|E
0 ED 9C 11 C3 6A E3 AB DA EF CF C0 AC F0 23 E7 7C |i|.Äjã«ÜiÄ-ð#ç|
0 17 C7 89 76 67 D9 CF A5 A8 00 00 00 00 49 45 4E |.ÇlvqÜi¥".IEN
0 44 AE 42 60 82 D@B' |
```

https://blog.csdn.net/qq_29647709

一共提权138位。

使用zlib进行压缩，代码如下：

```
#!/usr/bin/env python

import zlib

import binascii

IDAT = "789C5D91011280400802BF04FFFF5C75294B5537738A21A27D1E49CFD17DB3937A92E7E603880A6D485100901FB0410"

#print IDAT

result = binascii.hexlify(zlib.compress(IDAT))

print (result.decode('hex'))

print (len(result.decode('hex')))
```

得到压缩后的文件：



https://blog.csdn.net/qq_29647709

发现是626猜想是一个二维码的矩阵:

使用代码做成二维码:

代码如下:

```
from PIL import Image
from zlib import *

MAX = 25
pic = Image.new("RGB", (MAX, MAX))
str = "111111100010000110111111100000101110010110100001101110101000000001011101101110100100000001011"

i=0
for y in range(0, MAX):
    for x in range(0, MAX):
        if(str[i] == '1'):
            pic.putpixel([x, y], (0, 0, 0))
        else: pic.putpixel([x, y], (255, 255, 255))
        i = i+1
pic.show()
pic.save("flag.png")
```

运行得到二维码:

