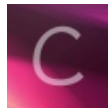


CryMisc__writeup

转载

zyxyzz 于 2017-05-22 19:40:04 发布 1828 收藏

分类专栏: [Write_up](#) 文章标签: [CryMisc-wp](#)



[Write_up](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

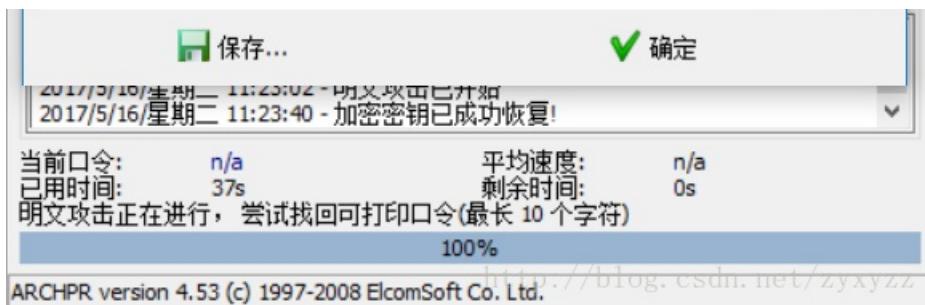
CryMisc__writeup

把CryMisc.zip解密后得到crypto.zip和jiami.py, crypto.zip是被加密过的, 而jiami.py则是加密脚本,

```
1 # -*- coding:utf8 -*-
2
3 import pyminizip
4 from hashlib import md5
5 import os
6
7 def create(files, zfile):
8     password = os.urandom(15)
9     password = md5(password).hexdigest()
10    pyminizip.compress_multiple(files, zfile, password, 0)
11    pass
12
13 if __name__ == '__main__':
14     files = ['jiami.py', 'gogogo.zip']
15     zfile = 'crypto.zip'
16     create(files, zfile) http://blog.csdn.net/zyxyzz
```

其中密码是随机的15位字符的md5值, 基本不可能爆破, 而这里是使用本身这个jiami.py和gogogo.zip一起加密成crypto.zip, 这里就存在着zip的明文攻击, 用winrar (不能用7zip或者好压) 把jiami.py压缩成jiami.zip, 使用archpr选择“明文攻击”





因为密码长度过长，导致无法直接获取到，但是点击“确定”可以另存为已经解密好的crypto_decrypted.zip，解压其中的gogogo.zip得到AESCrypt.py、AES.encrypt、RSA.encrypt，其中AESCrypt.py内容是模仿勒索软件，先AES加密，然后把key通过RSA进行加密。这里RSA文件只需要先分解即可，直接上脚本。

```

1 # -*- coding:utf8 -*-
2 from Crypto.Cipher import AES
3 import gmpy2
4
5 c=long(open('RSA.encrypt','rb').read().encode('hex'),16)
6 n=0x48D6B5DAB6617F21B39AB2F7B14969A7337247CABB417B900AE1D986DB47D971
7 e=0x10001
8 #通过yafu来分解n
9 p=185783328357334813222812664416930395483
10 q=177334994338425644535647498913444186659
11 d=gmpy2.invert(e,(p-1)*(q-1))
12 m=pow(c,d,n)
13 key='{ :x}'.format(m).decode('hex')
14
15 s=open('AES.encrypt','rb').read()
16 obj=AES.new(key,AES.MODE_ECB)
17 s=obj.decrypt(s)
18 BS=16
19 pad_len=ord(s[-1])
20 s=s[:-1*pad_len]
21 with open('next.zip','wb') as f:
22     f.write(s)

```

<http://blog.csdn.net/zyxyzz>

运行后可以得到AES的key为copy__white__key（这里也是稍微给后面的解密一点提示）、得到next.zip，解压后得到encrypt.py、first、second，其中encrypt.py就是对flag.jpg文件进行zip处理为2个文件。只要熟悉python代码，写个解密代码很简单。

```

1 # -*- coding:utf8 -*-
2 from base64 import *
3
4 s=[0,1]
5 with open('first','rb') as f:
6     s[0]=b16encode(f.read())
7 with open('second','rb') as f:
8     s[1]=b16encode(f.read())
9 s=map(''.join,zip(*s))
10 s=b16decode(''.join(s))
11 with open('flag.jpg','wb') as f:
12     f.write(s)

```

<http://blog.csdn.net/zyxyzz>

喂！老子在问你话啊！ 求婚戒指都准备好了 这段时间我过的很开心 看，妈妈，那是什么？
 等一切结束后，我有些话想跟你说 犯人也在我们之中，怎么可能一起睡！我回我自己房间去
 你看Jacky的鼻子很大对吧 哟！这位小哥匆匆忙忙要去哪儿啊？ 小西克幸 XXX由我来保护！
 谁敢杀我？谁敢杀我？谁敢杀我？ 才一个人也敢说出这种大话
 答应我，一定要好好活下去 这次的工作的报酬是以前无法比较的
 这里就交给我，你们快走！ 嗯？从未见过的武器？ 什么声音？去看一下吧
 自爆模式启动 明天是女儿的生日啊 我已经是天下无敌啦啦啦 顺便一提，我家的阳台不太稳固
 等这场战争结束，俺就要回老家结婚了！
 你这家伙是什么人？ 到了天竺之后，首先得把肚子填饱
 回想中 明天就去约她出来吧 什么嘛，原来是错觉
 区区人类 咦？... 怎么样？我说过没什么异常的吧 这次做完就金盆洗手
 已经死了么 CV很贵 嗯？老鼠么 成功了吗？ 这工作结束后我们两人一起生活吧
 我没想杀人，都、都是因为那家伙不好！全都是那家伙的错！所以我才【略
 吕、吕布啊啊啊啊啊啊啊啊啊啊！ 桑岛法子 大丈夫だ 问题ない
 叫破喉咙也不会有人来救你的
 原来是这么回事！得去告诉他们 放心，这艘船非常坚固，绝对不可能沉没的！

这里我为了容易做，使用了一张flag的百度百科上面的图片，如果可以细心的看到图片左下角的百度百科字样，去下载原图，然后对比后发现flag.jpg后面多出的数据其实是一个psd文件（原理是用copy命令把jpg文件和psd文件合并在一起）

```

UUU21F2U | B3 C9 73 24 91 CB F6 75 87 CB 89 8F CB 1E 17 AE | ^ESS LOUUEI E W
00021F30 | 39 E4 FA FA 0A 1B B8 1B B4 00 50 01 40 05 00 14 | 9aúú , ' P @
00021F40 | 00 50 01 40 05 00 7F FF D9 38 42 50 53 00 01 00 | P @ 8BPS
00021F50 | 00 00 00 00 00 00 03 00 00 01 90 00 00 01 90 00 |
00021F60 | 08 00 03 00 00 00 00 00 00 71 44 38 42 49 4D 04 | qD8BIM
00021F70 | 04 00 00 00 00 00 0F 1C 01 5A 00 03 1B 25 47 1C | Z %G
00021F80 | 02 00 00 02 00 00 00 38 42 49 4D 04 25 00 00 00 | 8BIM %
00021F90 | 00 00 10 CD CF FA 7D A8 C7 BE 09 05 70 76 AE AF | ííú}Ç% pv@
00021FA0 | 05 C3 4E 38 42 49 4D 04 24 00 00 00 00 3C B1 3C | ÅN8BIM $ <±<
00021FB0 | 3F 78 70 61 63 6B 65 74 20 62 65 67 69 6E 3D 22 | ?xpacket begin="
  
```

也可以通过8BPS头和8BIM字样推测是psd文件，用photoshop打开



最顶层的文字是假的，这里关键在于锁定的“背景”层，看似是新建图片时所留下的默认背景图，而本题就是把flag隐藏在里面，

把上面2层隐藏掉，然后对背景色另存为png格式（这样才能完好的保留颜色），使用stegsolve打开，并按下向左的按钮



就呈现出一幅二维码，扫描就得到flag{409d7b1e-3932-11e7-b58c-6807154a58cf}

这图的原理是前景色为(255,255,254)，人眼无法识别它跟白色的区别，而如果使用photoshop的油漆桶填充的时候，注意把默认的容差32改为容差0才可以看出区别。