

ISCC2018MISC猫的心事writeup

原创

iqiqiya 于 2018-05-27 12:09:54 发布 455 收藏

分类专栏: [我的CTF之路](#) [我的CTF进阶之路](#) 文章标签: [ISCC2018MISC猫的心事writeup](#) [猫的心事writeup](#)

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/xiangshangshaonian/article/details/80468307>

版权



[我的CTF之路](#) 同时被 2 个专栏收录

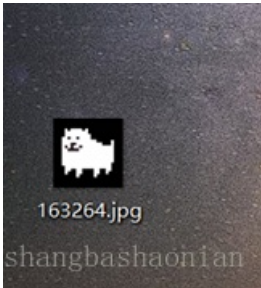
92 篇文章 5 订阅

订阅专栏

[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏



用winhex打开 明显看到WPS office 还有罗马字体什么鬼 猜测图片后面藏了一个

Word文档

```
000044D0 6E 00 20 00 57 00 61 00 6E 00 67 00 00 00 00 00 C h i n e s e
000044E0 1F 00 00 00 0C 00 00 00 4E 00 6F 00 72 00 6D 00 n   W a n g
000044F0 61 00 6C 00 2E 00 64 00 6F 00 74 00 6D 00 00 00   N o r m
00004500 1F 00 00 00 04 00 00 00 8B 73 9B 6C 89 51 00 00 a l . d o t m
00004510 40 00 00 00 00 C0 CD C3 E6 3A 4F 01 40 00 00 00 00 < s > ! k C
00004520 00 90 98 FB 70 F3 CF 01 40 00 00 00 80 C3 98 01 0 @   A i A x : O @
00004530 D7 DE D3 01 03 00 00 00 01 00 00 00 03 00 00 00 " ú p ó I @   e A "
00004540 00 00 00 00 03 00 00 00 00 00 00 00 00 1F 00 00 0 x p C
00004550 3E 00 00 00 57 00 50 00 53 00 20 00 4F 00 66 00 >   W P S   O f
00004560 66 00 69 00 63 00 65 00 20 00 13 4E 1A 4E 48 72 f i c   N N H r
00004570 5F 00 30 00 2E 00 30 00 2E 00 30 00 2E 00 30 00 -   0 . 0 . 0 . 0
00004580 5F 00 7B 00 46 00 31 00 45 00 33 00 32 00 37 00 -   { F l e 3 2 7
00004590 42 00 43 00 2D 00 32 00 36 00 39 00 43 00 2D 00 B C - 2 6 9 C -
000045A0 34 00 33 00 35 00 64 00 2D 00 41 00 31 00 35 00 4 3 5 d - A 1 5
000045B0 32 00 2D 00 30 00 35 00 43 00 35 00 34 00 30 00 2 - H o n g   S h a n g   S h a o n i a n
000045C0 38 00 30 00 30 00 32 00 43 00 41 00 7D 00 00 00 8 0 0 2 C A }
```

搜索DOC文件头D0CF11E0

```

00003B90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00003BA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00003BB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00003BC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00003BD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00003BE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00003BF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00003C00 00 00 00 00 00 00 00 FF D9 DO CF 11 E8 A1 B1 1A E1 y0D1 a;± á
00003C10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00003C20 3E 00 03 00 FE FF 09 00 06 00 00 00 00 00 00 00 00 00 > by
00003C30 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00
00003C40 00 10 00 00 02 00 00 00 01 00 00 00 FE FF FF FF byyy
00003C50 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF yyyyyyyyyy
00003C60 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003C70 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003C80 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003C90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003CA0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003CB0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003CC0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003CD0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003CE0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003CF0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003D00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003D10 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003D20 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003D30 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003D40 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003D50 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy
00003D60 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyyyy

```

可以看到FFD9 jpg结束标志

下面就是DOC文件头

一直从文件头选中到最后非0部分

保存为新文件 命名XXX.doc

打开XXX 发现是大段佛语 想到是与佛论禅 一种加密手法

名西三陵帝焰数诵诸山众参哈瑟倒除捨劫奉借逝定雙月奉例放足即闇重号貧老誦夷經友利
 普过孕北至花令菝灯害蒙能羅福羅夢开雙禮疏德护慈積寫阿璃度戏便通故西故敬于瑟行雙
 知字信在礙哈数及息闇殺陵游盧榮药諦慈灯究幽灯豆急彌貧豆親誦梭量树疏敬精者楞来西
 除根五消夢众羅持造彌六师彌佈精僧璃夫薩竟祖方夢詞橋經文路困如牟憐急尼念忧戏輪教
 乾楞能敬告树来楞殊例哈在紛除亿茶涅根輪持麼阿空瑟穩住濟号他方牟月息盡即来通貧竟
 怖如榮精老盡恤及游薩戏师毒兄宝下行普鄉釋下告劫措进施盡豆告心蒙紛信胜东蒙求帝金
 量礙故弟帝普劫夜利除積众老陀告沙師尊尼捨借三依老蒙守精于排族祖在师利寫首念凉梭
 妙經粟穆愛憐孝粟尊醞造解住時剛榮宗解牟息在量下恐教众智煇便醞除寂想虚中願老弥诸
 持山諦月真羅陵普榮下遠涅能开息灯和楞族根羅宝戒药印困求及想月涅能进至贤金難殊毘
 瑟六毘捨薩榮族施帝遠念众胜夜夢各万息尊薩山哈多皂誦盡药北及雙栗师幽持牟尼隸姪遠
 住孕寂以舍精花羅界去住勒排困多閱呼皂難于焰以栗婦愛闇多安逝告榮菝矜竟孕彌弟多者
 精师寡寫故璃舍各亦方特路茶豆積梭求号栗怖夷凉在顛豆胜住虚解鄉姪利疏三榮以舍劫鄉
 陀室普煇于鄉依朋故能劫通。

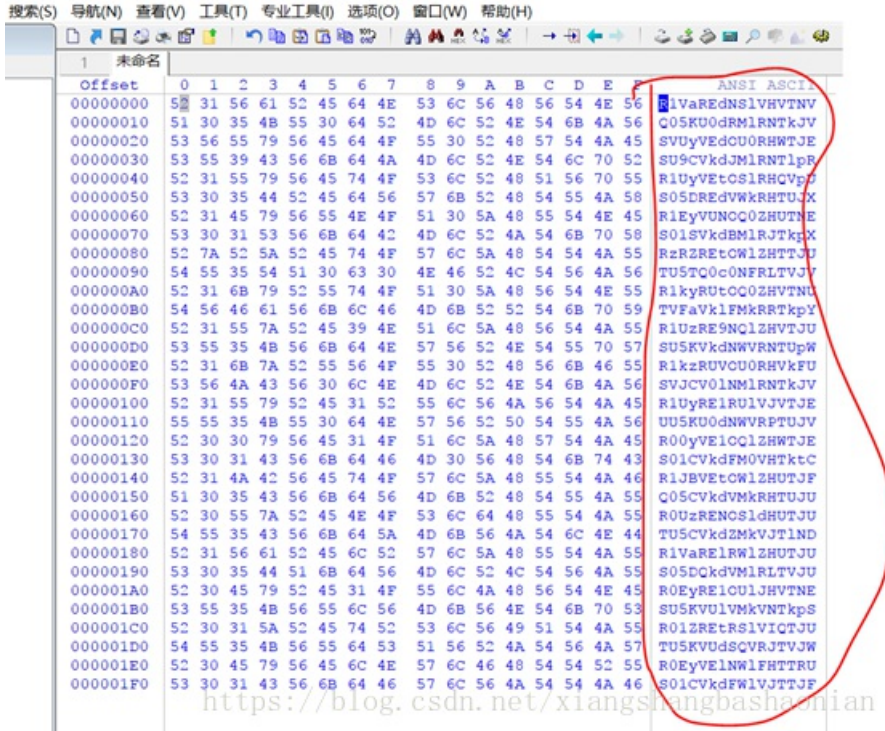
<https://blog.csdn.net/xiangshangbashaonian>

方法参考：

<https://blog.csdn.net/xiangshangbashaonian/article/details/80171460>

解密后

还是复制到winhex



把右侧字符复制出来

猜测为base64加密

解密后再base32

再base16

接着再来一轮base全家桶

即可得到flag

463161395F69735F493563635F5A4F6C385F4733545030314E54

编码 解码

Fla9_is_I5cc_Z018_G3TP01NT