【2020安洵杯】EasyCM WriteUp

原创

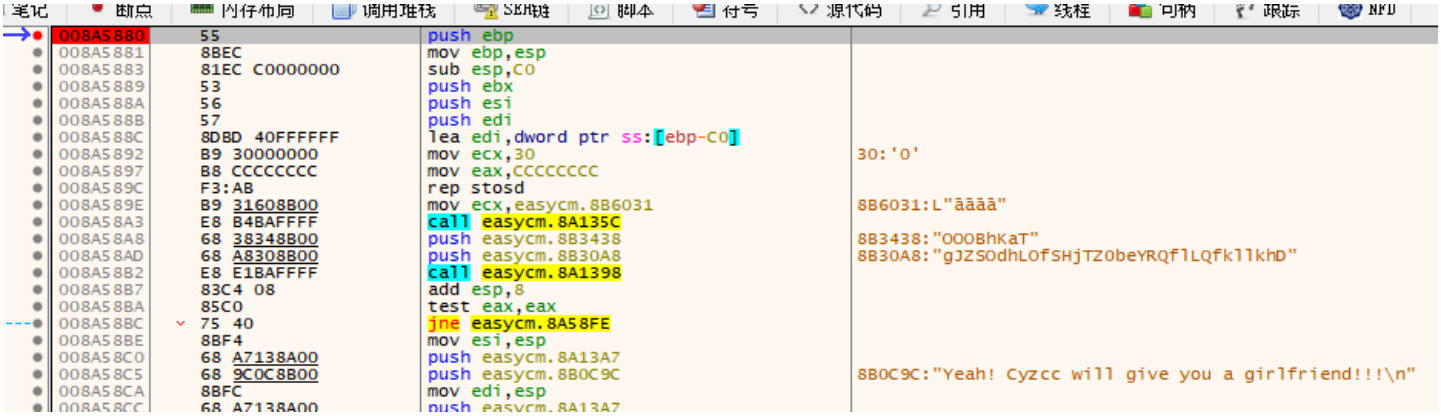
古月浪子 于 2020-12-17 23:39:41 发布 225 收藏 1

文章标签： CTF

本文链接：https://blog.csdn.net/tqydyqt/article/details/110123052

这题从早上9点开始，做了快3小时，最后被人领先8分钟拿了一血，只拿到一个二血，呜呜呜/(ㄒoㄒ)/~~

这题IDA有点白给，直接上x32dbg动调

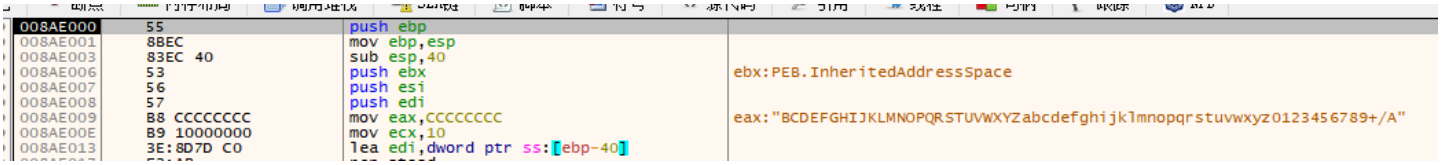


可以看到要比较的字符串

我输入的是111d0g，经过某种加密以后变成了OOOBhKaT

前面有判断输入是不是3的倍数，不是则用-补齐的操作

推测是3位一组，一组输出4个字符，有点像base64



加密操作在这个函数里，会调用length/3次，每次输出4个字符

这个函数是动态解密的，而且dump下来后idapython写IDA里patch后也没法F5，懒得修花指令了

读一读汇编能写出他的加密算法

解密脚本：

```
char table[] = "BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/A";

char getC1(char* s, int i)
{
 int idx = ((s[0] & 0xC0) | (s[1] & 0x30) | ((s[2] & 0x3) << 2)) >> 2;
 return table[(idx + i) % 64];
}

char getC2(char* s, int i)
{
 int idx = ((s[1] & 0xC0) | (s[2] & 0x30) | ((s[0] & 0x3) << 2)) >> 2;
 return table[(idx + i) % 64];
}

char getC3(char* s, int i)
{
 int idx = ((s[2] & 0xC0) | (s[0] & 0x30) | ((s[1] & 0x3) << 2)) >> 2;
 return table[(idx + i) % 64];
}

char getC4(char* s, int i)
{
 int idx = (((s[0] << 4) & 0xC0) | ((s[1] << 2) & 0x30) | (s[2] & 0xC)) >> 2;
 return table[(idx + i) % 64];
}

int main()
{
 char t[4];
 t[3] = 0;
 char flag[] = "gJZSOdhLOfSHjTZ0beYRQflLQfkllkhD";
 for (size_t i = 0; i < 32; i += 4)
  for (size_t j = 0; j < 128; j++)
   for (size_t k = 0; k < 128; k++)
    for (size_t l = 0; l < 128; l++)
    {
     t[0] = j;
     t[1] = k;
     t[2] = l;
     if (getC1(t, i / 4) == flag[i] && getC2(t, i / 4) == flag[i + 1] && getC3(t, i / 4) == flag[i + 2] && getC4
(t, i / 4) == flag[i + 3])
      cout << t;
    }
 return 0;
}
```