xctf BABYHOOK

原创

菜逼的ctf之路 于 2020-10-27 22:05:26 发布 68 收藏

xctf BABYHOOK

好几天没写了，该水一篇了
查壳(无壳，查过了)，看ida，主函数没有任何可疑的地方，但是因为添加了线程，所以猜测在线程中调用了核心函数，开始用ida动调，发现可疑的地方
在文件读取的地方调用了一个奇怪的函数

IDA View-A | Pseudocode-A | Hex View-1 | Structures | Enums | Imp

```
1  signed int __cdecl sub_401000(int a1, signed int a2)
2  {
3    char v2; // al
4    char v3; // bl
5    char v4; // cl
6    int v5; // eax
7
8    v2 = 0;
9    if ( a2 > 0 )
10   {
11     do
12     {
13       if ( v2 == 18 )
14       {
15         *(_BYTE *)(a1 + 18) ^= 0x13u;
16       }
17       else
18       {
19         if ( v2 % 2 )
20           v3 = *(_BYTE *)(v2 + a1) - v2;
21         else
22           v3 = *(_BYTE *)(v2 + a1 + 2);
23         *(_BYTE *)(v2 + a1) = v2 ^ v3;
24       }
```

```
19          if ( v2 % 2 )
20            v3 = *(_BYTE *)(v2 + a1) - v2;
21          else
22            v3 = *(_BYTE *)(v2 + a1 + 2);
23          *(_BYTE *)(v2 + a1) = v2 ^ v3;
24        }
25        ++v2;
26      }
27      while ( v2 < a2 );
28    }
29    v4 = 0;
30    if ( a2 <= 0 )
31      return 1;
32    v5 = 0;
33    while ( byte_40A030[v5] == *(_BYTE *)(v5 + a1) )
34    {
35      v5 = ++v4;
36      if ( v4 >= a2 )
37        return 1;
38    }
39    return 0;
40  }
00001015 sub_401000:17 (401015)
```


在动调看汇编的过程中发现这个函数会改变输入的字符串，盲猜是加密的核心函数，看代码是把输入的字符串按奇数和偶数区分。

如果是奇数：flag[i]=(a1[i]^i)+i

如果是偶数：flag[i+2]=(a[i]^i)

最后一位：flag[18]=a[18]^18

可以看出flag[0]没有被操作

所以写脚本

```
a= [
    0x61, 0x6A, 0x79, 0x67, 0x6B, 0x46, 0x6D,
    0x2E, 0x7F, 0x5F, 0x7E, 0x2D, 0x53, 0x56,
    0x7B, 0x38, 0x6D, 0x4C, 0x6E, 0x00
    ]
flag=list("1234567891234567890")
for i in range(18):
    if(i%2):
        flag[i]=chr((a[i]^i)+i)
    else:
        flag[i+2]=chr(a[i]^i)
print("".join(flag))
flag[18]=(a[18]^18)
```

得到结果把第一位赋值f字符就行了