xctf key

原创

酸酸菜鱼 于 2020-09-06 16:12:10 发布 202 收藏
分类专栏： CTF

CTF 专栏收录该内容
41 篇文章 1 订阅
订阅专栏

单看代码看不明白。动态调试了一波。答案都在注释里了。

- 程序计算出一个值，与文件里的值比较，相同即可

```
unsigned int sub_401100()
{
  signed int v0; // esi
  signed int v1; // esi
  unsigned int v2; // edi
  void **v3; // ebx
  void **v4; // eax
  int v5; // ecx
  int v6; // ST04_4
  int v7; // ST08_4
  int v8; // ST0C_4
  int v9; // eax
  char *v10; // esi
  int v11; // ecx
  void **v12; // eax
  signed int v13; // eax
  int v14; // ecx
  int v15; // eax
  int v16; // eax
  int v17; // eax
  int v18; // eax
  int v19; // eax
  int v20; // eax
  int v21; // eax
  const char *v22; // edx
  int v23; // eax
  unsigned int result; // eax
  int Dst; // [esp+14h] [ebp-124h]
  char v26[4]; // [esp+20h] [ebp-118h]
  char v27; // [esp+24h] [ebp-114h]
  int v28; // [esp+5Ch] [ebp-DCh]
  char v29; // [esp+61h] [ebp-D7h]
  int v30; // [esp+64h] [ebp-D4h]
  int v31; // [esp+68h] [ebp-D0h]
  char v32; // [esp+6Ch] [ebp-CCh]
  FILE *File; // [esp+70h] [ebp-C8h]
  char v34; // [esp+84h] [ebp-B4h]
  void *v35; // [esp+CCh] [ebp-6Ch]
  int v36; // [esp+DCh] [ebp-5Ch]
```

```
unsigned int v37; // [esp+E0h] [ebp-58h]
void *v38; // [esp+E4h] [ebp-54h]
unsigned int v39; // [esp+F4h] [ebp-44h]
unsigned int v40; // [esp+F8h] [ebp-40h]
void *Memory[4]; // [esp+FCh] [ebp-3Ch]
unsigned int v42; // [esp+10Ch] [ebp-2Ch]
unsigned int v43; // [esp+110h] [ebp-28h]
__int128 v44; // [esp+114h] [ebp-24h]
__int16 v45; // [esp+124h] [ebp-14h]
char v46; // [esp+126h] [ebp-12h]
int v47; // [esp+134h] [ebp-4h]

v40 = 15;
v39 = 0;
LOBYTE(v38) = 0;
v47 = 0;
v37 = 15;
v36 = 0;
LOBYTE(v35) = 0;
LOBYTE(v47) = 1;
v0 = 0;
v42 = 'dime';
LOWORD(v43) = 'a';
*(_OWORD *)Memory = xmmword_40528C;           // htadimehtadimeht
v45 = '.<';
v46 = 0;
v44 = xmmword_4052A4;                         // <<<....++++---->
do
{
  sub_4021E0(&v35, 1u, (*((_BYTE *)Memory + v0) ^ *((_BYTE *)&v44 + v0)) + 22);// *this, size_t Size, cha
  ++v0;
}
while ( v0 < 18 );                            // 循环计算后的结果：`[^VZe`uYaY]`s^joY
v1 = 0;
v43 = 15;
v42 = 0;
LOBYTE(Memory[0]) = 0;
LOBYTE(v47) = 2;
v2 = v37;
v3 = (void **)v35;
do
{
  v4 = &v35;
  if ( v2 >= 0x10 )
    v4 = v3;
  sub_4021E0(Memory, 1u, *((_BYTE *)v4 + v1++) + 9);// 循环后的结果：idg_cni~bjbfi|gsxb
}
while ( v1 < 18 );
memset(&Dst, 0, 0xB8u);
sub_401620(&Dst, v5, v6, v7, v8);             // 有打开文件的操作  在这之前是可以的  读取文件操作里没有操作内容
LOBYTE(v47) = 3;
if ( v26[*(_DWORD *)(Dst + 4)] & 6 )
{
  v9 = sub_402A00(std::cerr, "?W?h?a?t h?a?p?p?e?n?");// 传入，在下一行输出
  std::basic_ostream<char,std::char_traits<char>>::operator<<(v9, print);
  exit(-1);
}
sub_402E90(&Dst, &v38);                       // 获取内容
v10 = &v27;
if ( File )
if ( File )
{
  if ( !sub_4022F0(&v27) )
    v10 = 0;
  if ( fclose(File) )
    v10 = 0;
}
else
{
  v10 = 0;
}
v32 = 0;
v29 = 0;
std::basic_streambuf<char,std::char_traits<char>>::_Init(&v27);
v30 = dword_408590;
File = 0;
v31 = dword_408594;
v28 = 0;
if ( !v10 )
  std::basic_ios<char,std::char_traits<char>>::setstate((char *)&Dst + *(_DWORD *)(Dst + 4), 2, 0);
v12 = Memory;
if ( v43 >= 0x10 )
  v12 = (void **)Memory[0];
v13 = sub_4020C0(&v38, v11, v39, (int)v12, v42);// v42=0  比较函数。获取flag.txt里的值。与 idg_cni~bjbfi|gsx
v14 = std::cout;
if ( v13 )
{
  v22 = "=W=r=o=n=g=K=e=y=";
}
else
{
  v15 = sub_402A00(std::cout, "|------------------------------|");
  std::basic_ostream<char,std::char_traits<char>>::operator<<(v15, print);
  v16 = sub_402A00(std::cout, "|==============================|");
  std::basic_ostream<char,std::char_traits<char>>::operator<<(v16, print);
  v17 = sub_402A00(std::cout, "|==============================|");
  std::basic_ostream<char,std::char_traits<char>>::operator<<(v17, print);
  v18 = sub_402A00(std::cout, "|==============================|");
  std::basic_ostream<char,std::char_traits<char>>::operator<<(v18, print);
  v19 = sub_402A00(std::cout, "\\  /\\  /\\  /\\  /\\==============|");
  std::basic_ostream<char,std::char_traits<char>>::operator<<(v19, print);
  v20 = sub_402A00(std::cout, " \\/  \\/  \\/  \\/  \\=============|");
  std::basic_ostream<char,std::char_traits<char>>::operator<<(v20, print);
  v21 = sub_402A00(std::cout, "                 |-------------|");
  std::basic_ostream<char,std::char_traits<char>>::operator<<(v21, print);
  std::basic_ostream<char,std::char_traits<char>>::operator<<(std::cout, print);
  v14 = std::cout;
  v22 = "Congrats You got it!";
}
v23 = sub_402A00(v14, v22);
std::basic_ostream<char,std::char_traits<char>>::operator<<(v23, print);
sub_401570(&v34);
std::basic_ios<char,std::char_traits<char>>::~basic_ios<char,std::char_traits<char>>(&v34);
if ( v43 >= 0x10 )
  sub_402630(Memory[0], v43 + 1);
if ( v2 >= 0x10 )
  sub_402630(v3, v2 + 1);
result = v40;
if ( v40 >= 0x10 )
  result = sub_402630(v38, v40 + 1);
  return result;
}
```