攻防世界 gametime

原创

蚁小剑 于 2021-08-09 21:12:10 发布

分类专栏： CTF 文章标签： 游戏 算法 安全架构 安全

本文链接：https://blog.csdn.net/P_Bloomberg/article/details/119547037

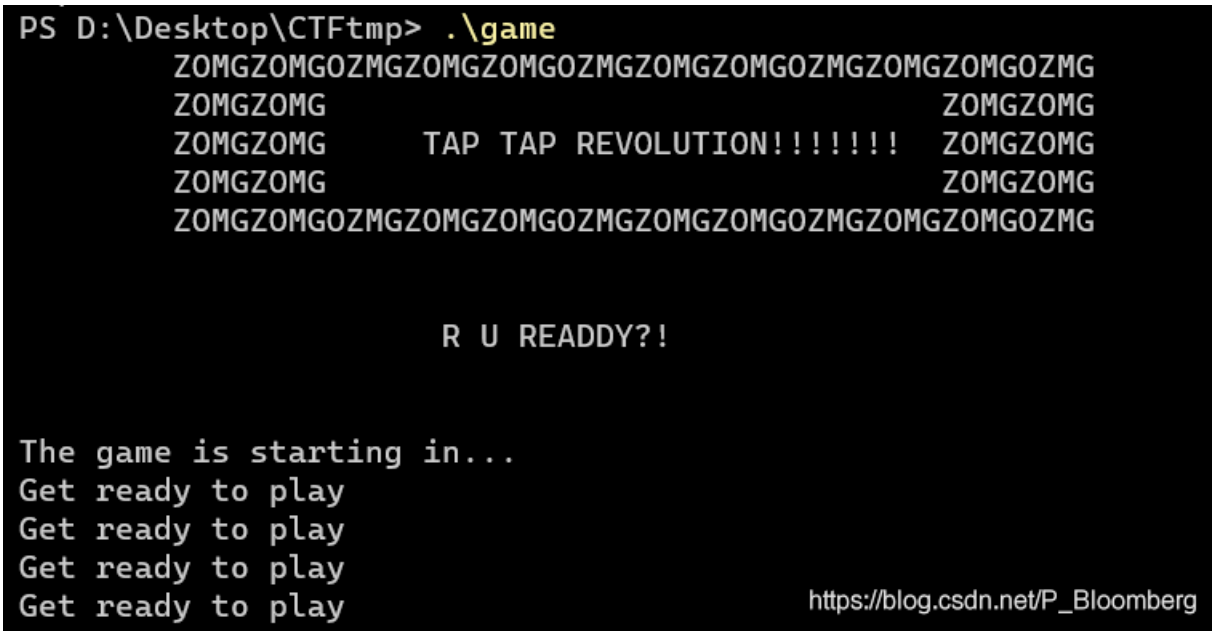
准备

工具：IDA、x32dbg、010Editor

环境：Windows10

开始

附件是exe可执行文件，在cmd里执行后，发现是一个游戏



玩了一会后，发现规律大概是它出现什么字母，你就要根据下面的规则按下相应的键

```
's'-->' '    'x'-->'x'    'm'-->'m'
```

一开始可能还可以，后来速度快就没法玩，所以动态调试

IDA静态分析

先拖进IDA中，分析main函数

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // edi
```

```
unsigned int v4; // eax
int v5; // ecx
int v6; // ecx
int v7; // ecx
void (__stdcall *v8)(DWORD); // ebx
int v9; // esi
int v10; // esi
int v11; // esi
int v12; // esi
int v13; // esi
int i; // edi
int v15; // esi
unsigned __int8 *v16; // esi
int v17; // ebx
int v18; // esi
int v19; // esi
char v20; // cl
int v22; // [esp+10h] [ebp-20h]
int v23; // [esp+14h] [ebp-1Ch] BYREF
char v24; // [esp+1Bh] [ebp-15h]
_WORD v25[3]; // [esp+1Ch] [ebp-14h] BYREF
int v26; // [esp+22h] [ebp-Eh]
int v27; // [esp+26h] [ebp-Ah]
__int16 v28; // [esp+2Ah] [ebp-6h]

strcpy((char *)v25, " ");
v23 = 7630702;
*(_DWORD *)&v25[1] = 0;
v26 = 0;
v27 = 0;
v28 = 0;
v3 = 0;
v22 = 0;
sub_401A73((int)"\r\tZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG\n");
sub_401A73((int)"\tkey is %s (%s)", (const char *)&v23, (const char *)v25);
sub_401423();
sub_401A73((int)"\r\tZOMGZOMG                                    ZOMGZOMG\n");
sub_401A73((int)"\tkey is %s (%s)", (const char *)&v23, (const char *)v25);
sub_401423();
sub_401A73((int)"\r\tZOMGZOMG     TAP TAP REVOLUTION!!!!!!  ZOMGZOMG\n");
sub_401A73((int)"\tkey is %s (%s)", (const char *)&v23, (const char *)v25);
sub_401423();
sub_401A73((int)"\r\tZOMGZOMG                                    ZOMGZOMG\n");
sub_401A73((int)"\tkey is %s (%s)", (const char *)&v23, (const char *)v25);
sub_401423();
sub_401A73((int)"\r\tZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG\n\n\n");
sub_401A73((int)"\tkey is %s (%s)", (const char *)&v23, (const char *)v25);
sub_401423();
sub_401A73((int)"\r\t              R U READDY?!\n\n\n");
sub_401A73((int)"\tkey is %s (%s)", (const char *)&v23, (const char *)v25);
sub_401423();
sub_401A73((int)"\rThe game is starting in...\n");
v4 = _time64(0);
srand(v4);
sub_4012B2();
sub_4012D5(0xC8u);
if ( !(unsigned __int8)sub_401435(10, v5, v25, &v23) )
  return 0;
if ( !(unsigned __int8)sub_401435(8, v6, v25, &v23) )
```

```
  return 0;
if ( !(unsigned __int8)sub_401435(5, v7, v25, &v23) )
  return 0;
sub_401A73((int)"key is %s (%s)", (const char *)&v23, (const char *)v25);
sub_401A73((int)"\rTRAINING COMPLETE!                              \n");
v8 = Sleep;
v9 = 20;
do
{
  Sleep(0xC8u);
  sub_401A73((int)"\n");
  --v9;
}
while ( v9 );
sub_401A73((int)"key is %s (%s)", (const char *)&v23, (const char *)v25);
sub_401A73((int)"\rNow you know everything you need to know");
v10 = 4;
do
{
  sub_401A73((int)".");
  Sleep(0x3E8u);
  --v10;
}
while ( v10 );
sub_401A73((int)"\n\n\nfor the rest of your life!\n");
v11 = 20;
do
{
  Sleep(0xC8u);
  sub_401A73((int)"\n");
  --v11;
}
while ( v11 );
sub_401A73((int)"LETS PLAY !\n");
v12 = 20;
do
{
  Sleep(0xC8u);
  sub_401A73((int)"\n");
  --v12;
}
while ( v12 );
sub_4012B2();
sub_4012D5(0x64u);
if ( !(unsigned __int8)sub_401507(0xC8u, (int)v25, (int)&v23) )
  return 0;
if ( !(unsigned __int8)sub_401507(0xC8u, (int)v25, (int)v25) )
  return 0;
if ( !(unsigned __int8)sub_401507(0xC8u, (int)v25, (int)v25) )
  return 0;
sub_401A73((int)"key is %s (%s)", (const char *)&v23, (const char *)v25);
sub_401423();
sub_401A73((int)"\rooooh, you fancy!!!\n");
if ( !(unsigned __int8)sub_401507(0xC8u, (int)v25, (int)&v23)
  || !(unsigned __int8)sub_401507(0xC8u, (int)v25, (int)&v23)
  || !(unsigned __int8)sub_401507(0xC8u, (int)v25, (int)&v23) )
{
  return 0;
}
sub_401A73((int)"key is %s (%s)", (const char *)&v23, (const char *)v25);
```

```
  sub_401A73((int)"\b\b");
  sub_401A73((int)"NIIICE JOB)!!!!\n");
  v13 = 20;
  do
  {
    Sleep(0x32u);
    sub_401A73((int)"\n");
    --v13;
  }
  while ( v13 );
  v24 = 1;
  do
  {
    if ( v3 % 3 == 1 )
    {
      sub_401A73((int)"key is %s (%s)", (const char *)&v23, (const char *)v25);
      sub_401423();
      sub_401A73((int)"\rTURBO TIME!    \n");
      for ( i = 0; i < 20; ++i )
      {
        v8(0x32u);
        sub_401A73((int)"\n");
        if ( i == 19 )
        {
          v15 = sub_40141D();
          sub_401D02(v25, v15 - 5514);
          dword_41A1F8 = (int)v25;
          dword_41A1FC = v15 - 5498;
          sub_401AA5();
          sub_401CC9();
          sub_401A73((int)"key is %s (%s)", byte_417D02, (const char *)&v23);
          sub_401A73((int)"\b\b");
          v16 = (unsigned __int8 *)v25;
          v17 = 16;
          do
          {
            sub_401A73((int)"%02x", *v16++);
            --v17;
          }
          while ( v17 );
          sub_401A73((int)")\n\n");
          v8 = Sleep;
        }
      }
      v18 = 0;
      while ( 1 )
      {
        rand();
        if ( !(unsigned __int8)sub_401507(0x64u, (int)v25, (int)&v23) )
          break;
        if ( ++v18 >= 10 )
          goto LABEL_33;
      }
      v24 = 0;
LABEL_33:
      v3 = v22;
    }
    v19 = 0;
    while ( 1 )
```

```
    {
      rand();
      v20 = v24;
      if ( v24 )
        break;
LABEL_38:
      if ( ++v19 >= 10 )
        goto LABEL_41;
    }
    if ( (unsigned __int8)sub_401507(0x64u, (int)v25, (int)&v23) )
    {
      v20 = v24;
      goto LABEL_38;
    }
    v20 = 0;
    v24 = 0;
LABEL_41:
    if ( v3 == 1337 )
    {
      sub_4012F6();
      v20 = v24;
    }
    v22 = ++v3;
  }
  while ( v20 );
  return 0;
}
```

代码很长，分析关键部分

第60行到第66行是教你怎么玩，函数是sub_401435()

```
char __usercall sub_401435@<al>(DWORD a1@<edx>, int a2@<ecx>, int a3, int a4, const char *a5, const char *a6)
{
  int v8; // edi

  sub_401A73((int)"key is %s (%s)", a6, a5);
  sub_401423();
  sub_401A73((int)"\rZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG\n");
  if ( a2 == 32 )
    sub_401A73((int)"\nWhen you see an 's', press the space bar\n\n");
  else
    sub_401A73((int)"\nWhen you see an '%c', press the '%c' key\n\n", a2, a2);
  sub_401A73((int)"key is %s (%s)", a6, a5);
  sub_401423();
  sub_401A73((int)"\rZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG\n");
  sub_4012D5(a1);
  v8 = a3;
  if ( a3 > 0 )
  {
    do
    {
      sub_401A73((int)".");
      Sleep(0xC8u);
      --v8;
    }
    while ( v8 );
  }
  if ( sub_401260(a2, 100000) ) //关键
    return 1;
  sub_401A73((int)"key is %s (%s)\r", a6, a5);
  sub_401423();
  sub_401A73((int)"\rUDDER FAILURE! http://imgur.com/4Ajx21P \n");
  return 0;
}
```

从第98行开始就是自己玩，函数是sub_401507()

```
char __usercall sub_401507@<al>(int a1@<edx>, int a2@<ecx>, DWORD dwMilliseconds, int a4, int a5)
{
  sub_401A73((int)"key is %s (%s)", (const char *)a5, (const char *)a4);
  sub_401423();
  sub_401A73((int)"\r                                    \r");
  if ( a1 > 0 )
  {
    do
    {
      sub_401A73((int)".");
      Sleep(dwMilliseconds);
      --a1;
    }
    while ( a1 );
  }
  if ( sub_401260(a2, 500 * dwMilliseconds) ) //关键
    return 1;
  sub_401A73((int)"key is %s (%s)\r", (const char *)a5, (const char *)a4);
  sub_401A73((int)"UDDER FAILURE! http://imgur.com/4Ajx21P \n");
  return 0;
}
```

可以看出游戏里面的关键函数都是sub401260()，只要它返回值为1，游戏就会进行下去，否则就会输出

```
sub_401A73((int)"UDDER FAILURE! http://imgur.com/4Ajx21P \n");
```

分别查看sub_401435()、sub_401507()两个函数中调用sub401260()的位置

· sub_401435()

```
.text:004014CA                mov     edx, 186A0h
.text:004014CF                mov     ecx, esi
.text:004014D1                call    sub_401260
.text:004014D6                pop     edi
.text:004014D7                pop     esi
.text:004014D8                pop     ebx
.text:004014D9                test    al, al
.text:004014DB                jnz     short loc_401503
.text:004014DD                push    [ebp+arg_8]
```


在004014D1处调用，在004014DB时判断返回结果

· sub_401507()

```
.text:00401551 loc_401551:                            ; CODE XREF: sub_401507+31↑j
.text:00401551                imul    edx, edi, 1F4h
.text:00401557                mov     ecx, ebx
.text:00401559                call    sub_401260
.text:0040155E                pop     edi
.text:0040155F                pop     esi
.text:00401560                pop     ebx
.text:00401561                test    al, al
.text:00401563                jnz     short loc_401586
.text:00401565                push    [ebp+arg_4]
.text:00401568                push    [ebp+arg_8]
```


在00401559处调用，在00401563时判断返回结果

所以破解方案就是，在这两处判断的地方打上断点，修改ZF标志位，使它原来的跳转指令朝着相反的方向执行。（即不执行）

动态调试

动态调试之前，要使用010Editor关掉aslr，具体方法参照博客

[(30条消息) 攻防世界 Windows_Reverse1_P_Bloomberg的博客-CSDN博客]的动态调试部分。

修改之后

将文件放入x32dbg中先按下F9开始，指令地址就会变得和IDA中相同

再在004014DB和00401563两处打上断点。

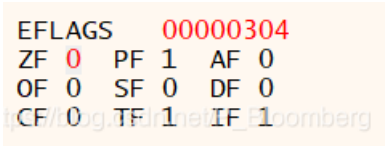
```
00401560   5B          pop ebx
00401561   84C0        test al,al
00401563   75 21       jne game.401586
00401565   FF75 0C     push dword ptr ss:[ebp+C]
00401568   FF75 10     push dword ptr ss:[ebp+10]      [ebp+10]:"not"
```

```
004014D7   5E          pop esi
004014D8   5B          pop ebx
004014D9   84C0        test al,al
004014DB   75 26       jne game.401503
004014DD   FF75 10     push dword ptr ss:[ebp+10]      [ebp+10]:"not"
004014E0   FF75 14     push dword ptr ss:[ebp+14]
004014E3   68 707A4100 push game.417A70                417A70:"key is %s (%s)\r"
```

然后一直F9执行，执行到断点处时，修改sub401260()的返回结果

```
EFLAGS   00000344
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1
```

即修改EFLAGS中的ZF标志位，改成与原来相反的数即可



执行一段时间后，大概是在main函数的153行处，就会输出完整的flag

运行过程：

```
        ZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG
        ZOMGZOMG                                  ZOMGZOMG
        ZOMGZOMG     TAP TAP REVOLUTION!!!!!!!    ZOMGZOMG
        ZOMGZOMG                                  ZOMGZOMG
        ZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG


                     R U READDY?!


The game is starting in...
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
ZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG

When you see an 's', press the space bar

ZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
.........s
ZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG

When you see an 'x', press the 'x' key

ZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
```

```
Get ready to play
Get ready to play
Get ready to play
........x
ZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG

When you see an 'm', press the 'm' key

ZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMGZOMGZOMGOZMG
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
.....m
TRAINING COMPLETE!
```

```
Now you know everything you need to know....


for the rest of your life!
```

```
LETS PLAY !
```

```
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
Get ready to play
.....s
..x
.m
ooooh, you fancy!!!
.....m
..x
.s
key is not (NIIICE JOB)!!!!
```

```
....x
....x
.....m
.....m
....x
...s
...s
....x
.....m
....x
TURBO TIME!
```

```
key is  (no5c30416d6cf52638460377995c6a8cf5)
```

flag：`no5c30416d6cf52638460377995c6a8cf5`