看雪 2016CrackMe 攻防大赛 - 1-Crack_Me-凉飕飕

原创

什么名字都被用了 于 2018-10-15 10:49:31 发布 909 收藏

分类专栏： 看雪 2016CrackMe 攻防大赛 文章标签： CrackME

本文链接：https://blog.csdn.net/goodnameused/article/details/83055666

看雪 2016CrackMe 攻防大赛 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

环境：

Windows xp

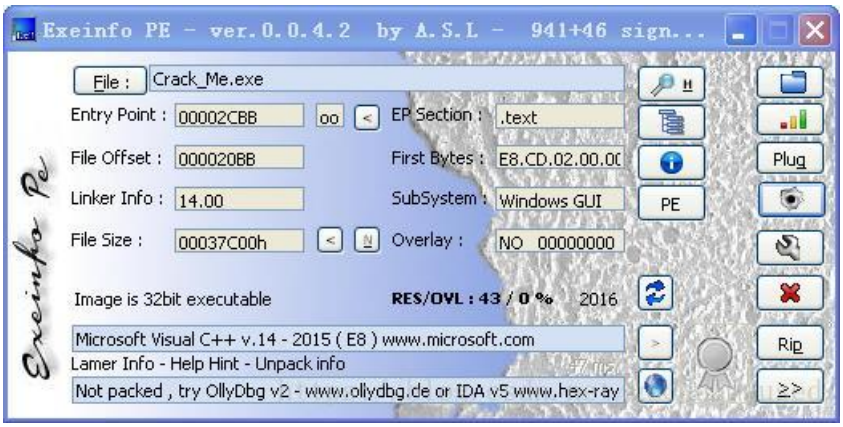
工具：

IDA

EXEINFOPE

OD

0x00 查壳



EXEINFOPE查壳，

无壳

0x01 分析

```
  if ( (unsigned __int16)wParam == 0x40B )    // 成功
  {
    *(_OWORD *)v22 = xmmword_41DB98;
    v25 = 0;
    v23 = xmmword_41DBA8;
    v24 = xmmword_41DBB8;
    memset_4039D0(&v26, 0, 150);
    MessageBoxW(hWnd, v22, L"Successed", 0);
    return 0;
  }
  if ( (unsigned __int16)wParam == 0x40C )
  {
    sub_402970((_WORD *)lParam, &v21);
    v9 = (_WORD *)sub_402CD6(2 * (v21 + 1) | -((unsigned __int64)(unsigned int)(v21 + 1) >> 31 != 0));
    strcpy_402870((int)v9, (_WORD *)lParam);
    sub_4029B0(v9);
    sub_402A00(v9);
    memset_4039D0((_BYTE *)v22, 0, 200);
    strcpy_402870((int)v22, v9);
    release_402CDF(v9);
    v10 = 0;
    if ( v22[0] )
    {
      v11 = 0;
      v12 = v22;
      do
      {
        ++v10;
        *v12 ^= *(_WORD *)(v11 + lParam);
        v11 = 2 * v10;
        v12 = &v22[v10];
      }
      while ( *v12 );
    }
    if ( sub_402810((char *)lParam, (char *)v22) )
      SendMessageW(hWnd, 0x111u, 0x40Au, 0);
    return 0;
  }
  if ( (unsigned __int16)wParam == 1039 )     // 0x40F
  {
    MessageBoxW(0, L"something you lost!", L"Failed", 0);
    return 0;
  }
  return DefWindowProcW(hWnd, 0x111u, wParam, lParam);
}
if ( (unsigned __int16)wParam == 0x40A )
{
  *(_OWORD *)Text = xmmword_41DB60;
  v28 = xmmword_41DB70;
  v29 = xmmword_41DB80;
  _mm_storel_epi64((__m128i *)&v30, _mm_loadl_epi64((const __m128i *)&qword_41DB90));
  memset_4039D0(&v31, 0, 44);
  MessageBoxW(hWnd, Text, L"Failed", 0);
  return 0;
}`
```

可知wParam == 0x40B时弹出成功对话框。

```
if ( a1 )
{
  if ( a2 )                                     // 第2次调用时执行这里
  {
    v8 = debug_4048DE();
    memset_4039D0(&String, 0, 200);
    GetWindowTextW(*((HWND *)v2 + 3), &String, 200);// 读取输入内容
    v4 = 0;                                     // 输入内容长度
    v5 = &String;
    if ( String )
    {
      do
      {
        ++v5;
        ++v4;
      }
      while ( *v5 );
    }
    v6 = (_WORD *)sub_402CD6(2 * (v4 + 1) | -((unsigned __int64)(v4 + 1) >> 31 != 0));
    if ( debug_4048DE() - v8 > 2 )              // 猜测是测试是否在被调试
    {
      sub_404BB1();
      JUMPOUT(*(_DWORD *)byte_401E45);
    }
    strcpy_402870((int)v6, &String);            // v6是个地址，输入内容长度xor0x5
    if ( v4 >= 7 )
    {
      if ( v4 <= 7 )                            // 输入内容长度是否为7
      {
        sub_401A60((int)v2, v6);                // 下一关
        return;
      }
      v7 = 0x40D;
    }
    else
    {
      v7 = 0x40E;
    }
    SendMessageW(*((HWND *)v2 + 1), v7, 0, 0);
    release_402CDF(v6);
    return;
  }
  if ( sub_401C00(a1)                           // 检查输入内容是否含有'b'
    && (memset_4039D0(&String, 0, 200),
        GetWindowTextW(*((HWND *)v2 + 3), &String, 100),
        sub_402A50(v3, (__int16 *)&String, 'p')) )// 检查输入内容是否含有'p'
  {
    sub_401CB0(v2, 1);
  }
  else
  {
    SendMessageW(*((HWND *)v2 + 1), 0x111u, 0x40Fu, 0);
  }
}
```

首先是判断输入内容里是否含有'b'、'p'这两个字符
然后再判断输入内容长度是否为7

```
 do
    {
      v18 = v3[v17];
      if ( v18 >= 0x61 && v18 <= 0x7A )
        v3[v17] = v18 - 32;
      ++v17;
    }
    while ( v17 < v15 );                        // 输入内容小写字母转大写
  }
```

```
do
  {
    if ( v20 )
    {
      v23 = *v22;                               // 输入内容
      v24 = v33;                                // A-Z
      v25 = 0;
      while ( v23 != *v24 )                     // 判断输入的字符是否在表中
      {
        v24 = &v33[++v25];
        if ( !v33[v25] )                        // 是否超出A-Z范围
          goto LABEL_37;
      }
      *(_WORD *)v21 = v33[v25];                 // 在范围里的话就保存起来
      v21 = (__int64 *)((char *)v21 + 2);
LABEL_37:
      v20 = v33[0];
    }
    v22 = &v3[++v19];                           // 下一个字符
  }
  while ( v3[v19] );
```

如果输入的内容是字母就保存起来。

```
v27 = &v35;                             // 提取出来的字符
if ( (_WORD)v35 )
{
  do
  {
    v27 = (__int64 *)((char *)v27 + 2);
    ++v26;
  }
  while ( *(_WORD *)v27 );
  if ( v26 == 2 )                       // 如果有两个字符是在表中
  {
    LODWORD(v35) = 0x350031;            // 这里确定了输入内容第3位到第6位只能是15pb
    HIDWORD(v35) = &unk_420050;
    v28 = v3 + 2;
    v36 = 0;
    v29 = 0;
    while ( *((_WORD *)&v35 + v29) == *v28 )
    {
      ++v29;
      ++v28;
      if ( v29 >= 4 )
      {
        if ( !sub_401740((_DWORD *)v2, v3) )  // v2尝试次数
          break;
        v31 = 0x40B;
        return PostMessageW(*(HWND *)(v2 + 4), 0x111u, v31, 0);// 成功
      }
    }
  }
}
v31 = 0x40A;
return PostMessageW(*(HWND *)(v2 + 4), 0x111u, v31, 0);
```

统计输入内容是字母的个数，不等于2个就错误。
然后将输入内容与常数值比较，不满足也错误。

```
do
{
  *(_WORD *)v4 = v5;
  v4 = (__int128 *)((char *)v4 + 2);          // 将1-9放入v4
  ++v5;
}
while ( v5 <= 0x39 );
v6 = 0;
v7 = v2;
if ( v2 && *v2 )
{
  do
  {
    ++v7;
    ++v6;                                     // 计算输入长度
  }
  while ( *v7 );
}
v8 = sub_4028D0((char *)&v20, &v2[*v3]);      // 将1-9和输入的内容拼接，开始位置为尝试的次数
v9 = &v2[v6 - 1];                             // 取最后一个字符
v19 = v8;
v10 = 0;
v17 = v9;
```

```
  if ( (_WORD)v20 )
  {
    v11 = (char *)&v20;
    v12 = *v9 & 1;
    while ( 1 )
    {
      v13 = v12 + (*(_WORD *)v11 >> 2);
      if ( v13 == 0x32 )
        break;
      if ( v13 != 0x64 )
      {
        v11 = (char *)&v20 + 2 * ++v10;          // 下一个字符
        if ( *(_WORD *)v11 )
          continue;
      }
      v8 = v19;
      goto LABEL_12;
    }
  }
  else
  {
LABEL_12:
    v14 = &v20;
    v15 = 0x31;
    while ( *(_WORD *)v14 == *(_WORD *)((char *)v14 + (char *)v2 - (char *)&v20) )// 判断输入的第1个字符是否为1，
                                                 // 第2个字符是否为2，由此可知前6个字符为1215pb
    {
      v15 += 6;
      v14 = (__int128 *)((char *)v14 + 2);
      if ( v15 > 0x39 )
      {
        if ( *v2 + *((_WORD *)v8 + 9) == 0x63 && *v17 == *v18 + *((_WORD *)v8 + 6) )// v8[9]=='2' && s[6]==v8[6]
+尝试次数，v8[6]必定为7，
                                                 // v8[9]为输入内容[尝试次数]，由上面可知这个尝试次数必定为1
                                                 // 则s[6]必定为'8'，故结果为1215bp8
          return 1;                              // 一定要返回1
        return 0;
      }
    }
  }
```