2016 年第 7 题

大家好，我是胡一米。这期视频是关于 2016 年看雪 CTF 第 7 题解题资料。

一、简介

1.1 录制说明

视频是基于其他大佬文字 Writeup 录制的，所以在视频操作之前就已知了该题中的各种坑，如反调试等，所以不再演示踩坑过程。

1.2 录制参考

第 7 题主要参考了作者本文的叙述、HighHand、风间仁的 Writeup，链接如下：

风间仁：
https://bbs.pediy.com/thread-213966.htm

HighHand:
https://bbs.pediy.com/thread-213981.htm

1.3 内容简介

在本期中，主要讨论 2 个问题。这 2 个问题可能与最终的 Key 没有太大的联系，但题目中既然出现了，还是说一说。此 2 个问题分别是：
a. 通过 SEH 异常执行核心代码
b. 两人取数和最大，递归搜索

二、视频操作

2.1 静态分析定位关键点

结合其他大佬的分析过程，可以直接定位到关键点。.

类似的都是通过 SEH 触发异常来执行关键代码

Patch 的方法在 29 题有说到。

2.2 动态调试其加密过程

通过动态调试，理解程序的递归含义。

```
ll Sum(int i, int j,ll sum[maxn][maxn])
{
        if (i>j)return 0;
        if (~sum[i][j])return sum[i][j];
        if (i == j)return sum[i][j] = p_num[i];
        return sum[i][j] = (ll)p_num[i] + Sum(i + 1, j,sum);
}

ll dfs(int i,int j,ll dp[maxn][maxn] ){
        if (i>j)return 0;
        if (~dp[i][j])return dp[i][j];
        if (i == j)return dp[i][j] = p_num[i];

        return dp[i][j] = Sum(i, j,sum) - min(dfs(i, j - 1,dp), dfs(i + 1, j,dp));
}
```

博弈问题

941rPYOWMF3C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C69BKAKAKAKAKAKAKAKAKAKAKAKAKK8AE614

141622224F224C48C6n522GM6M2822C82822221F2eII2AUGig264w284ICIl1242M262G226S2Icq6A6o442

2.3 验证码与多解问题

使用 visual studio，编译作者的注册机，即可得到正确的注册码。

至于出现多解的原因有 2 个：其一是在验证 key 时，由一个博弈问题变成取数问题，这就导致了更多种的取法；其二是取法(flag)到 key 的转换方法不唯一。具体叙述如下：

以下所说的 flag 都是风间仁 writeup 中的 flag，具体含义是：为 1 则代表被取了；为 0 代表没有被取走。

风间仁通过递归搜索，得到了某一个 flag。总共的 flag 有 330 个，但是风间仁只取了其中的某一个。

但是这一个 flag 转换成 key 的方法不是唯一的。
如风间仁转化为：
941rPYOWMF3C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C69BKAKAKAKAKAKAKAKAKAKAKAKAKK8AE614。
其实也可以转换为：
941rPaOUMF3C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C2C69BKAKAKAKAKAKAKAKAKAKAKAKAKK8AE614。

这两个 key，都对应同一个 flag，也就是对应同一个递归解法。换句话说：flag 和 key 是一对多的关系。这就导致了每个 flag 可能对应多个 key。进一步地，又存在多个 flag，这使得 key 的数量会更多。在这么大范围的 key 中选择一个第 10 位为 F 的，同样存在很多。
0101
10101010101010101010101010101

0101101010101010101010101010101010101010101010101010101010101

三、小结

题目很好。