2016 年第 14 题

大家好，我是胡一米。这期视频是关于 2016 年看雪 CTF 第 14 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 14 题主要参看了 HighHand 和风间仁的 Writeup，链接如下：
HighHand:
https://bbs.pediy.com/thread-214298.htm
风间仁：
https://bbs.pediy.com/thread-214272.htm

1.3 内容简介

在本期中，主要讨论 1 个问题。这 1 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 1 个问题分别是：
a. Application Compatibility Database

二、视频操作

2.1 静态分析

a. Application Compatibility Database
https://msdn.microsoft.com/zh-cn/library/bb432182.aspx

https://www.microsoft.com/en-us/download/details.aspx?id=7352

2.2 动态调试程序逻辑

acdabaabbbccbbbbbbaaadccccaddaaazzzzzzzz
acddbccabcddacdbcdcbbadccaaddbcasojhyqq

1.
(v234 + 2 * (v231 + 2 * (v229 - 0x60 + 2 * v228 - 0x30) - 0x48)) ==5

v234 + 2*v231 + 4 * (v229 - 0x60 + 2 * v228 - 0x30) – 0x90 == 5

v234 = 1
v231 = 0
v229 = 1
v228 = 0

v233 + 2 * (v235 + 2 * (v232 - 0x60 + 2 * v230 - 0x30)) - 0x90 == 1

v233 = 1
v235 = 0
v232 = 0
v230 = 0

2.
31 00 30 00 31 00 31 00 30 00 30 00 30 00 30 00 31 00 31 00
10110000011

3.
v220 + 2 * (v219 + 2 * (v218 + 2 * v217)) - 0x2DB

v220 + 2 * v219 + 4 * v218 + 8 * v217 - 0x2DB = 8

v220 + 2 * v219 + 4 * v218 + 8 * v217 = 0x2DE
v220 = 0
v219 = 1
v218 = 1
v217 = 1

2.3 完成分析

最后，根据 acd_b 与 1.1.1.0.1.0.0.0 的对应关系，可以确定
a = 01
b = 00
c = 11
d = 10
注意，第一个 a 并没有参与编码。

三、小结

题目很好。

附录：

录制顺序：29-28-7-19-22-16-15-14-？