unity3d游戏IL2CPP相关算法简单分析

原创

点击上方↑↑↑蓝字[**协议分析与还原**]关注我们

“ 学习unity3d游戏的算法逆向。”

大家应该有印象，之前为分析菠菜应用，我写过简单的cocos2d游戏的逆向：

cocos2d游戏jsc文件格式解密，SpideMonkey大冒险

博彩应用奥迪棋牌协议破解分析与揭秘

途游斗地主加密协议分析及破解

最近接触了一些Unity3D的游戏的逆向，这是一个不同的游戏分支，在这里与大家分享分享，本篇纯技术说明，有机会再用实际游戏来探讨。

说到Unity3D，这是一个用得非常广的游戏引擎，当然，不局限于游戏。市面上很多游戏都是使用这个引擎，官网说Unity3D游戏的月下载量在好几十亿的级别。

例如这个游戏：

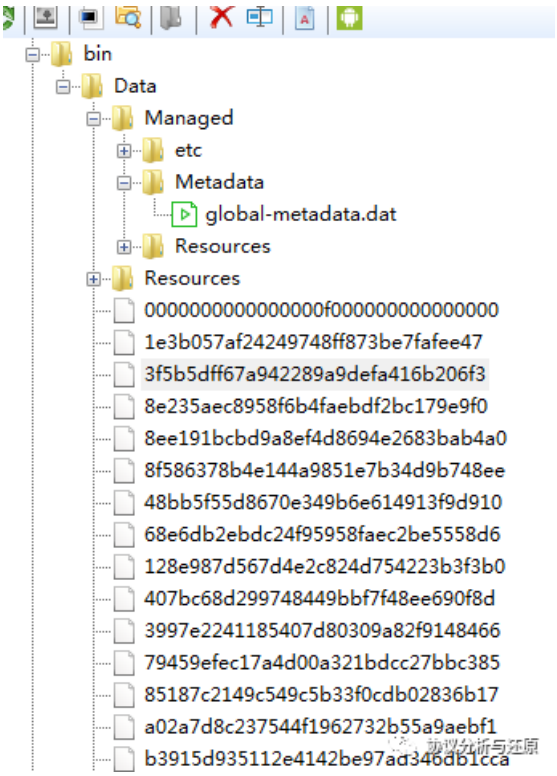
而IL2CPP，则是当前Unity3D游戏引擎的核心，具体大家去查阅相关文章啦，这里就不详细写了，对游戏逆向来说，IL2CPP包含了游戏的具体实现算法，分析一个游戏，基本上就是在分析IL2CPP这个库，例如，在Android平台，就是分析libil2cpp.so。

01

—

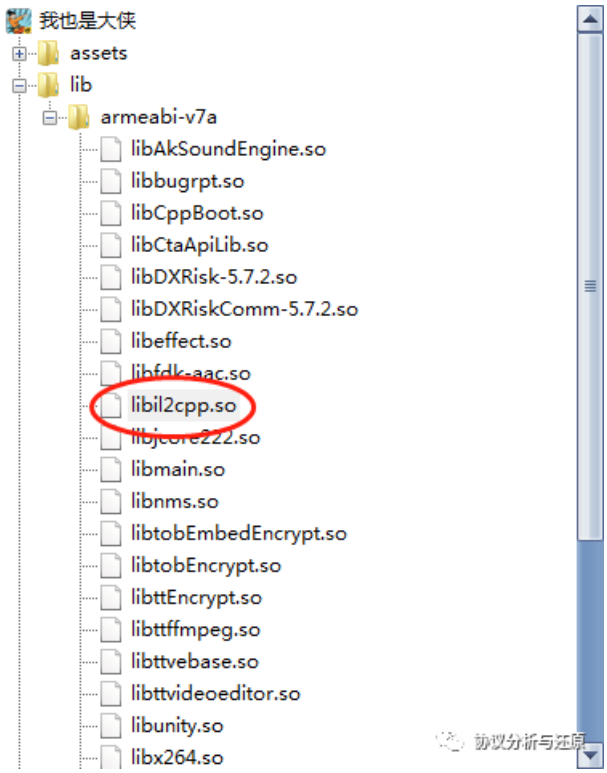
怎么分析

Android平台的Unity3D游戏，解包后会看到如下assert/bin/Data目录和文件：



其中global-metadata.dat是资源文件主体，与下面的哈希值为名称的文件建立关系。

另外还有so库目录下的libil2cpp.so库文件：



这个文件相当于游戏的具体实现，里面读取global-metadata.dat，并访问哈希值命名文件，以获取字符串等资源。

一般IL2CPP的Unity3D游戏的逆向，只需要根据global-metadata.dat和libil2cpp.so来进行就可以了，理论上，将libil2cpp.so这个库的函数，一个个看，总能找到想要的算法函数。

当然，没必要这样看对不对，嘻嘻。

对没有加固的IL2CPP Unity3D游戏，有一个非常方便的工具——Il2CppDumper，用起来很简洁，可以配合IDA将函数名变得有意义起来，不再是单调的sub_xxx，可以加快定位速度，当然，你也可以配合ILSpy之类的NET工具来用。

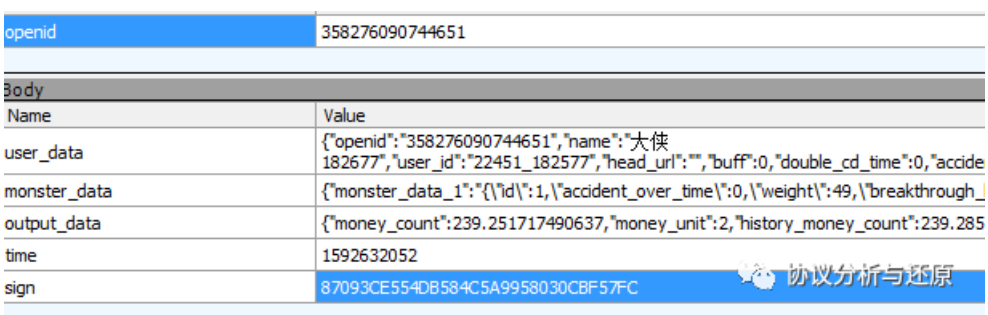
搞逆向的人多了，IL2CPP的Unity3D游戏就进入了加固的时代，常有两种加密方式，一种是libil2cpp.so的加壳，一种是global-metadata.dat的加密，这个就变得复杂了，没有一定之规，得一步步跟，一步步调，很花时间和精力，不是大的游戏的话，分析都有些不划算，这里不展开了。

02

—

一些经验之谈

好多的IL2CPP游戏，里面的实现逻辑都很类似。都是HTTP或HTTPS承载，URL参数里面带校验，这种，一般就是加盐的MD5啦，只是salt稍有不同，如果能使用Il2CppDumper的话，那只要找到相关的MD5函数，hook即可，用Frida就够了，例如这种：



如果不能Il2CppDumper，而global-metadata.dat又加密了，但libil2cpp.so没加壳的话，可以把libil2cpp.so全转出伪码，再根据算法的特征数，全文搜一下，嗖嗖几下，就能定位到需要的地方了，当然，要有耐心。

这个就写到这了，蛮枯燥的，希望对大家有帮助。

别忘点“在看”、“赞”和“分享”

新的规则，及时收推文要先给公号星标

别忘了星标一下，不然就错过了

长按进行关注，时刻进行交流。