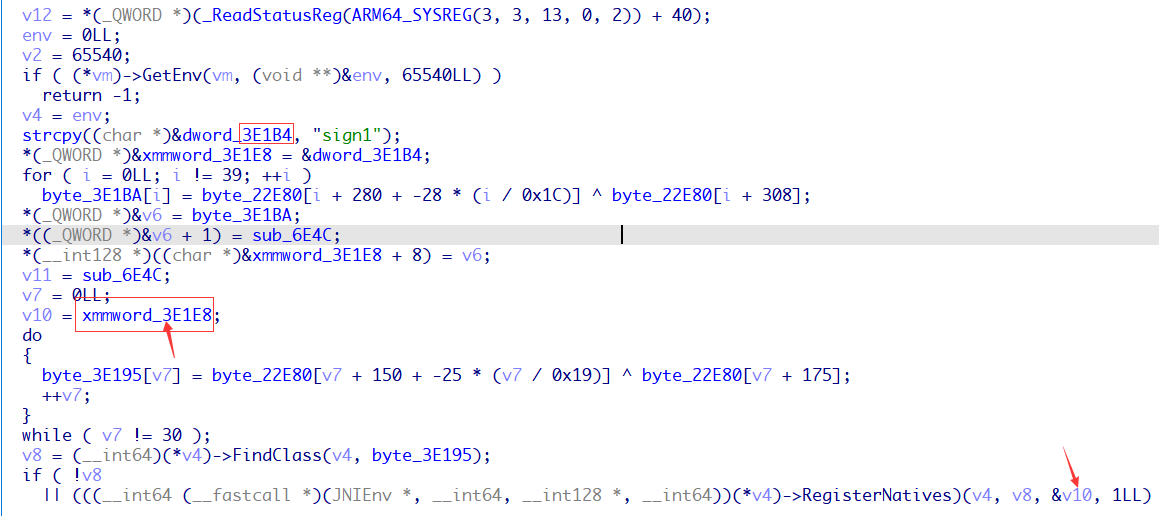
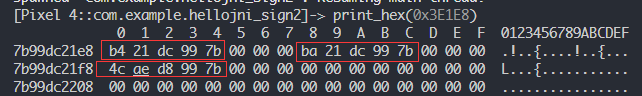
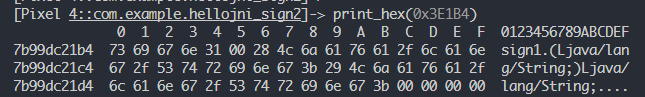
1. 这次的没有被ollvm加密字符串，不过在jni\_onload中用一些计算恶心了一下。其实还是可以直接hook RegisterNatives函数，不过这里我们手动看一下，熟悉下内存结构。



V10指向0x3E1E8，这三个地址其实就代表了函数名、签名和地址。这里可以看到第一个地址0x7b99dc21b4，其实就是被写入sign1字符串的bss段xmmword\_3E1B4

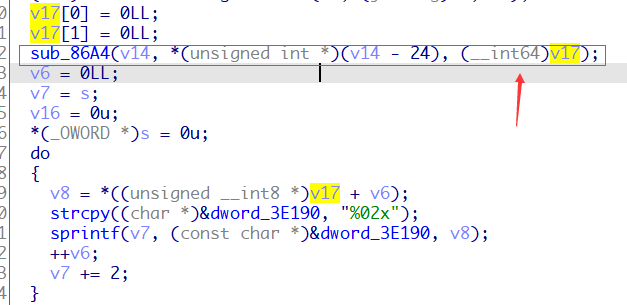




第三个是地址函数地址



1. 根据输出的交叉引用，快速定位到sub\_86A4，a3是result，a1是输入

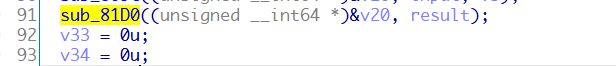




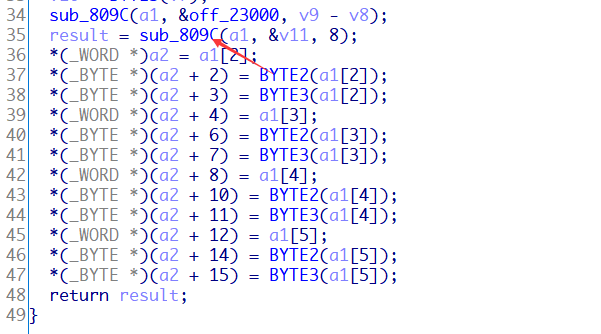
1. 这一串是拼接输入



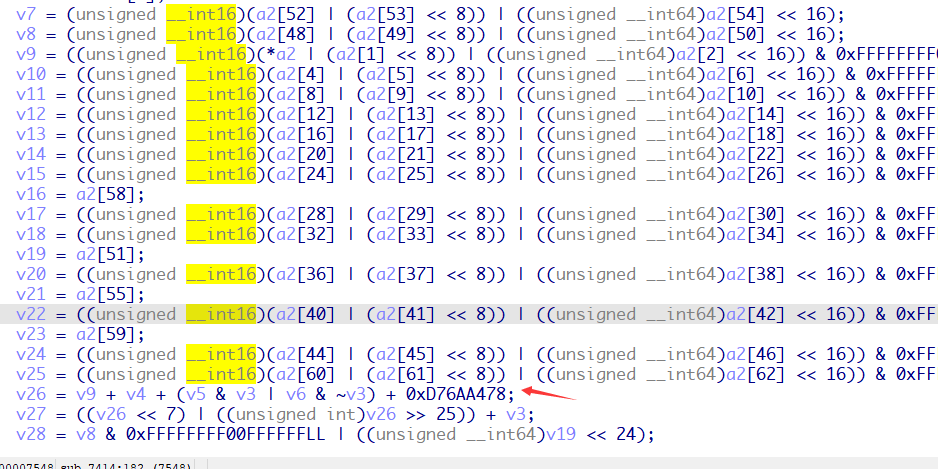
1. 还是倒着找，第一个关键函数sub\_81D0



之后是sub\_809c



在sub\_809c中，调用sub\_7414，MD5算法



1. Hook验证一下

