**校内通协议不完整分析**

moonflow --2012.8.22

校内通聊天加密部分的逆向分析，逆向需要学习的东西太多了。

       校内通采用开放的Jabber协议，在Jabber通信会话中，客户端和服务器协商使用TLS协议通信。TLS会话主要协商通信的加密方式、认证方式，为后面的数据通信提供安全的通道。

这个是Jabber通信的Jabber xml

                                                73  74 72 6561 6d 3a 73 74   ..h...<s tream:st

0040  72 6561 6d 20 74 6f 3d  22 74 61 6c 6b 2e 7265   ream to= "talk.re

0050  6e 7265 6e 2e 63 6f 6d  22 20 78 6d 6c 3a 6c61   nren.com" xml:la

0060  6e 673d 22 65 6e 22 20  76 65 72 73 69 6f 6e3d   ng="en"  version=

0070  22 312e 30 22 20 78 6d  6c 6e 73 3a 73 74 7265   "1.0" xm lns:stre

0080  61 6d3d 22 68 74 74 70  3a 2f 2f 65 74 68 6572   am="http ://ether

0090  78 2e6a 61 62 62 65 72  2e 6f 72 67 2f 73 7472   x.jabber .org/str

00a0  65 616d 73 22 20 78 6d  6c 6e 73 3d 22 6a 6162   eams" xm lns="jab

00b0  62 65 72 3a 63 6c 69 65  6e 74 22 3e 0d 0a         ber:clie nt">..

在聊天过程中，接收的信息是加密的。

000002AA  17 03 01 00 70 38 20 6f  68 84 39 d9 38 ba c2 98 ....p8 o h.9.8...

000002BA  0e 2b b2 c9 24 39 99 f5  e8 5c 59 c0 4f 9d 8c 70 .+..$9.. .\Y.O..p

000002CA  75 af 75 fc 2e 33 a5 64  85 b2 87 0f 84 bf f8 84 u.u..3.d ........

000002DA  f9 cd 44 b1 6c cd ff f8  e2 6e 72 d6 34 27 d7 1d ..D.l... .nr.4'..

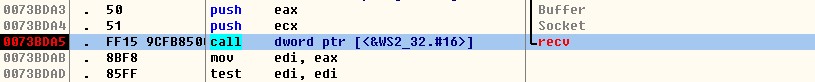
000002EA  10 2e f3 69 a2 d2 38 53  82 b7 b8 fa 7e 31 77 a3 ...i..8S ....~1w.

000002FA  33 a4 71 80 14 61 6c d9  2b f0 76 d8 4d ea 87 6c 3.q..al. +.v.M..l

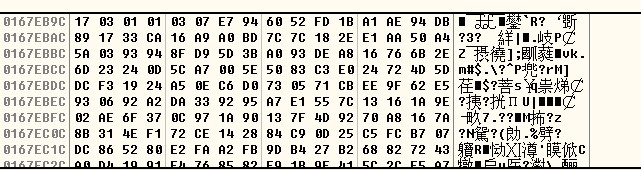
0000030A  27 b2 61 70 34 11 2b cf  fe 15 74 c2 0c 88 6e 1f '.ap4.+. ..t...n.

0000031A  7d f2 b3 af b1                                   }....

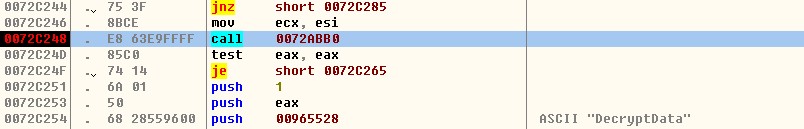
OD 加载校内通，在recv部分设置断点后，动态调试并查看数据内存部分变化



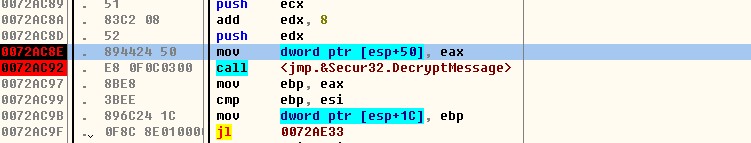
会发现此时buffer中就是上面以17 03 01开头的密文，这是ssl加密标识



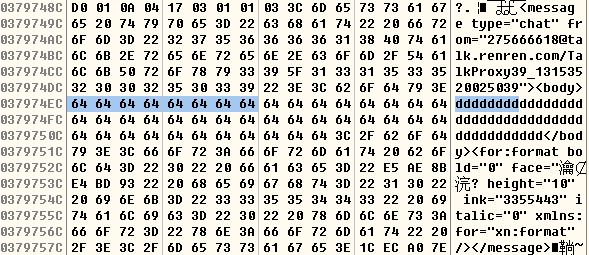
逐步调试，跟到了这个地方，F7进去



此时内存中还是密文



经过DecryptMessage后，内存中明文出现了



会发现明文部分数据ddddddddddddddddddddddddd

DecryptMessage貌似文档蛮少的，密钥的获取存在一定的难度，主要是要是RSA加密的话就歇菜了。

点到为止