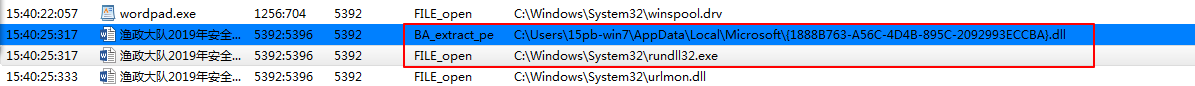
# 海莲花样本分析

平台：win7 32位

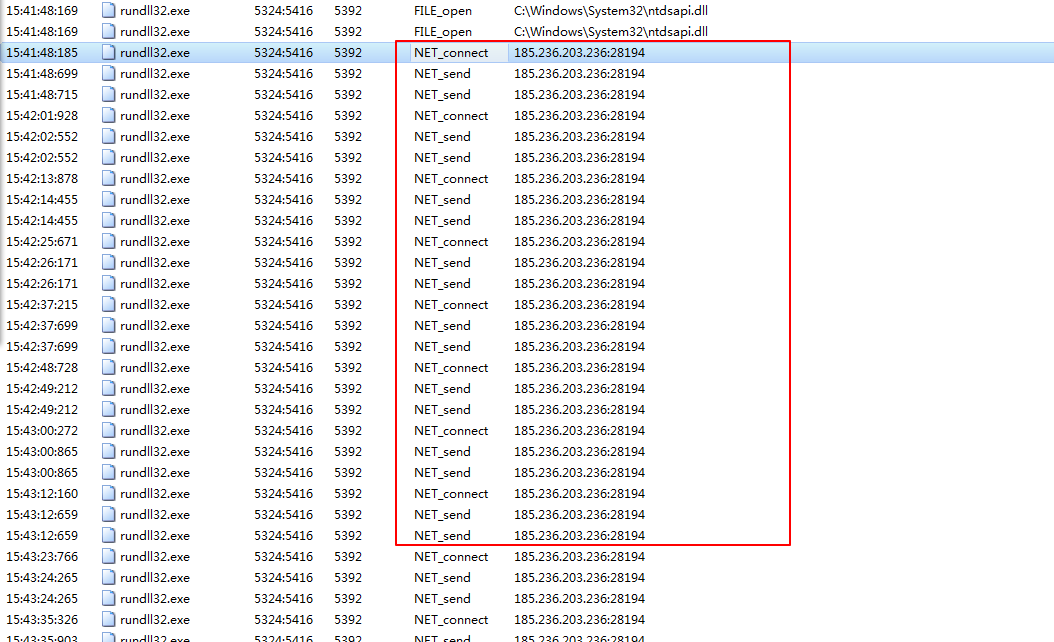
工具：IDA、OD、火绒剑、Fakenet等。。

## 资料搜集：

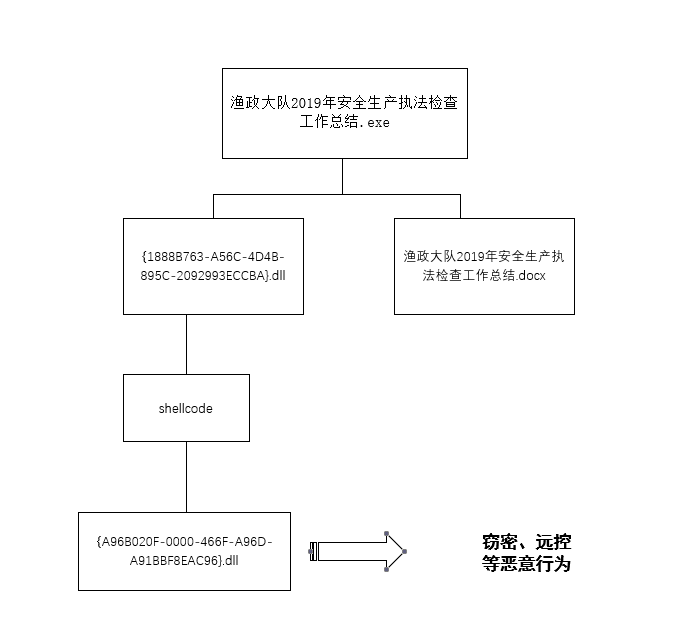
通过火绒剑检测行为发现样本exe释放了一个.docx和一个.dll文件，并执行了注册表以及网络连接等操作，接下来我们来详细调试一下看病毒文件具体是怎么执行这些操作的。



释放{1888B763-A56C-4D4B-895C-2092993ECCBA}.dll，并执行



进行网络连接和数据发送



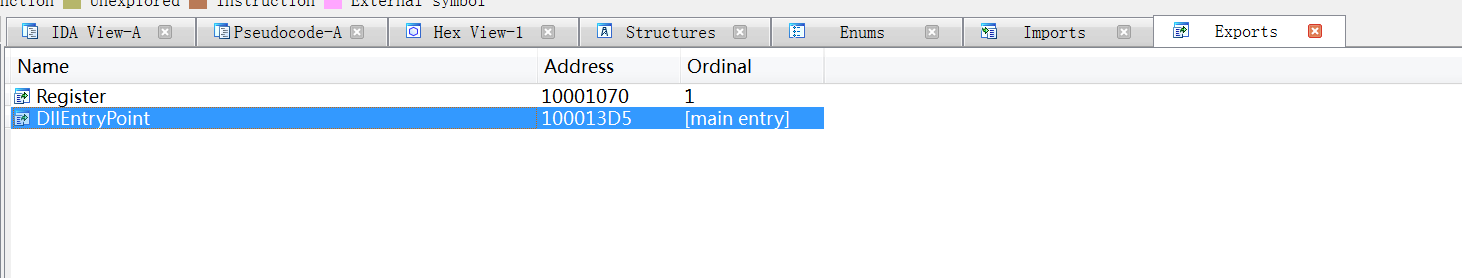
样本执行流程

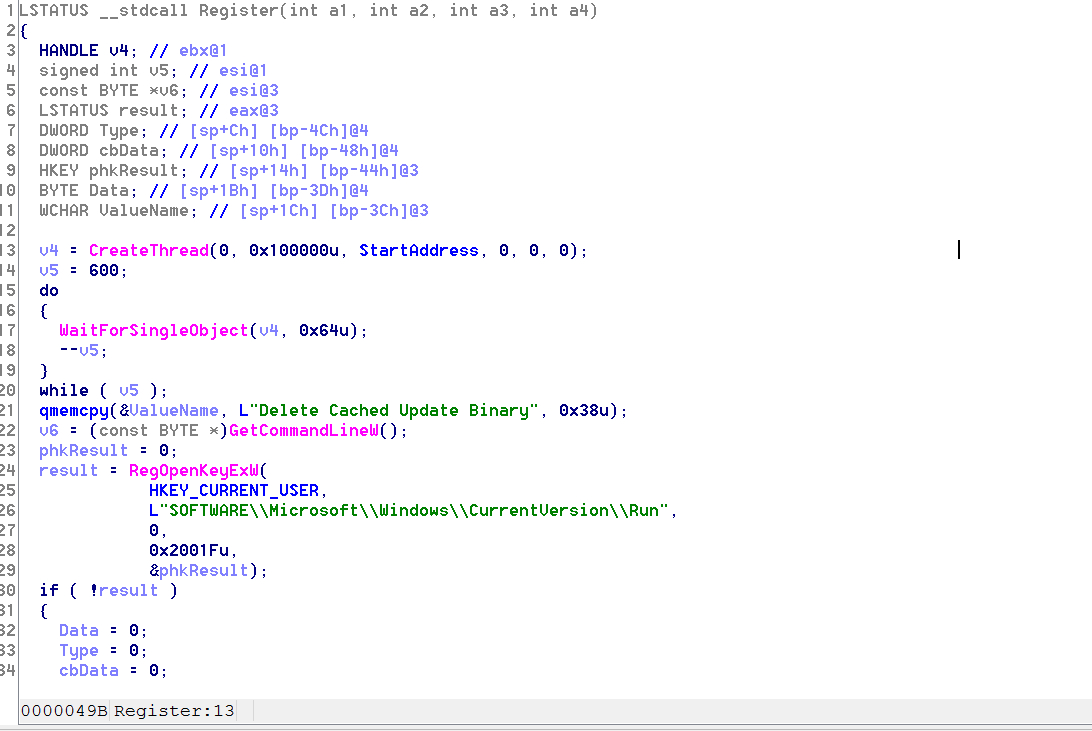
## 行为分析：

0x00 通过ida查看样本exe，发现其释放了一个Word文件和一个dll文件。并用命令行的方式启动rundll32.exe加载{1888B763-A56C-4D4B-895C-2092993ECCBA}.dll执行。

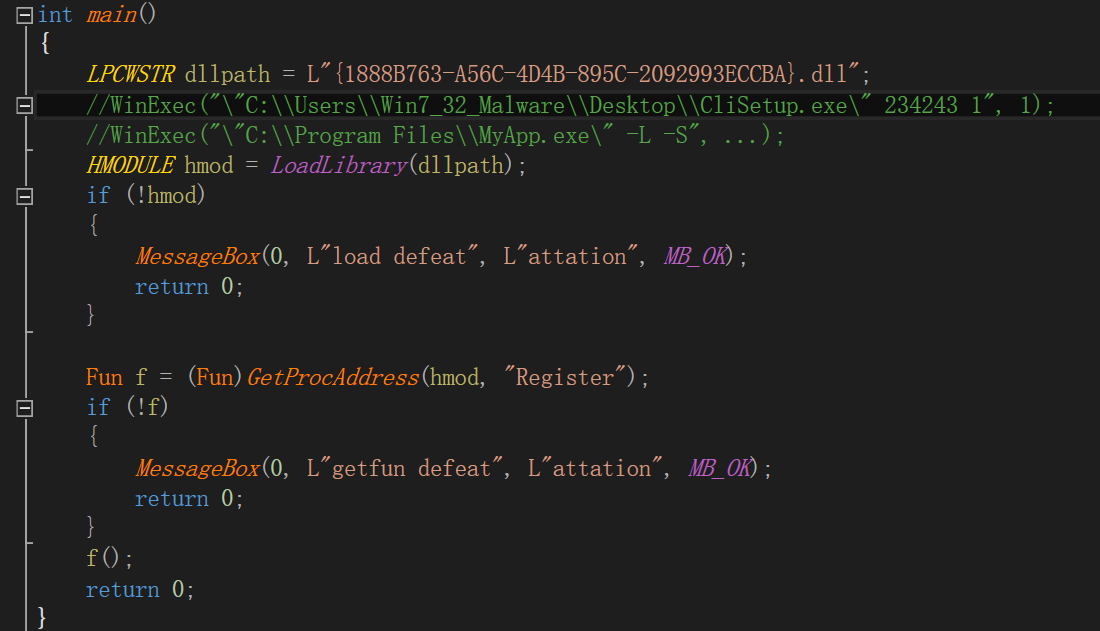


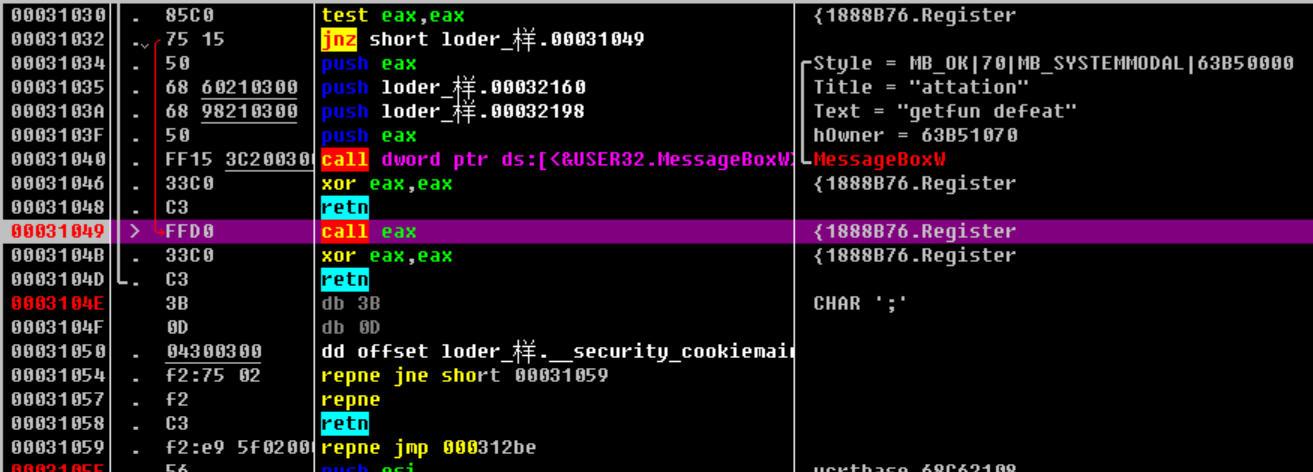
## 0x01 用ida分析释放的{1888B763-A56C-4D4B-895C-2092993ECCBA}.dll发现其有两个导出函数，DllEntry函数基本上没做什么操作，释放shellcode解密dll等操作都是在Register函数里面做的。





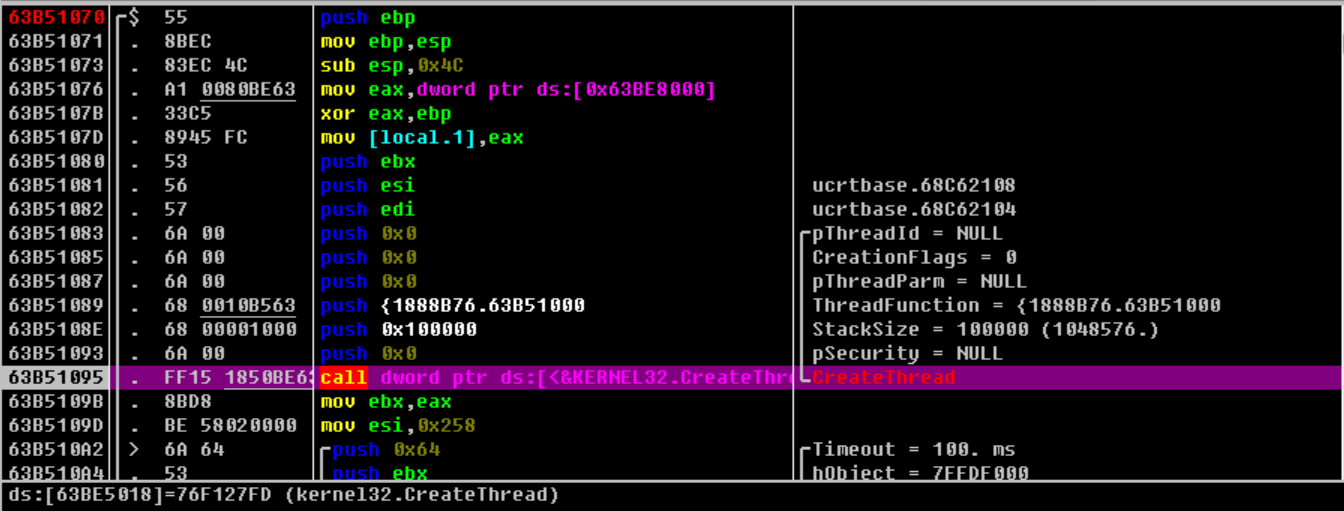
## 0x02 这样我们可以写个脚本直接执行Regiedit函数来调试会方便很多



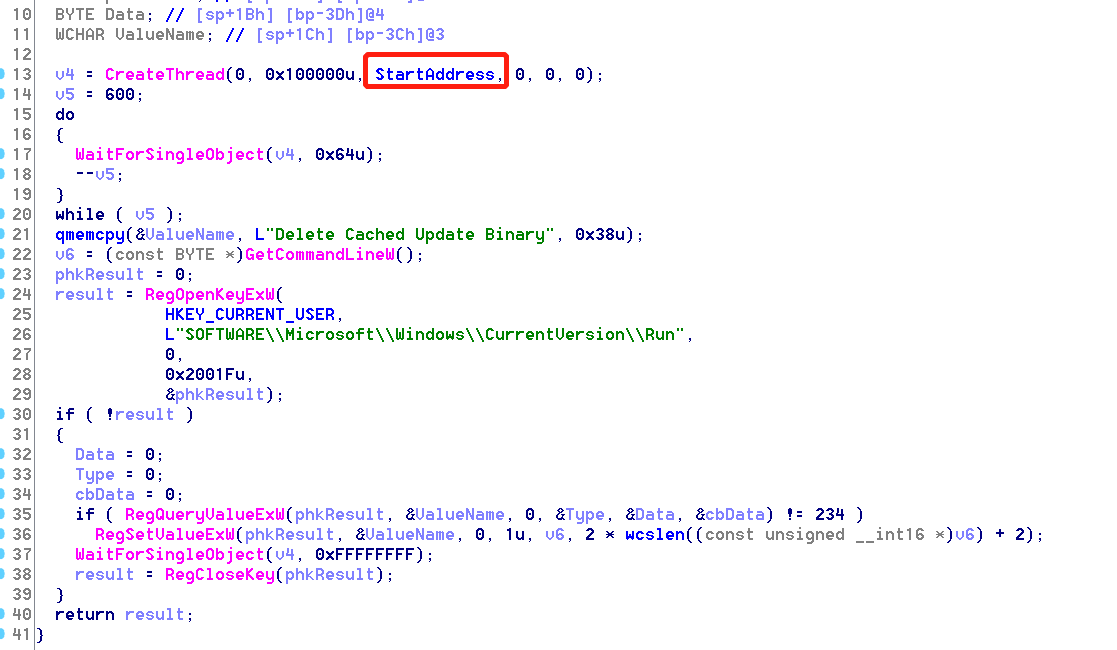


## 0x03 开始详细分析

3.1 进来之后看到了创建线程函数CreateThread

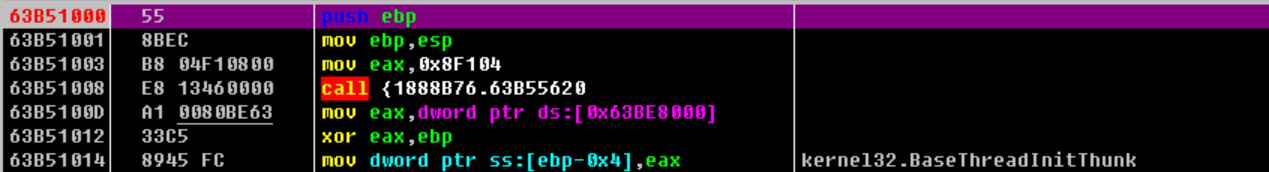


3.2 通过IDA查看Register函数结构猜测病毒的工作大部分是在CreateThread.ThreadFunction（0X63B51000）处操作的，所以我们可以主要从这个地址开始进行进一步分析。

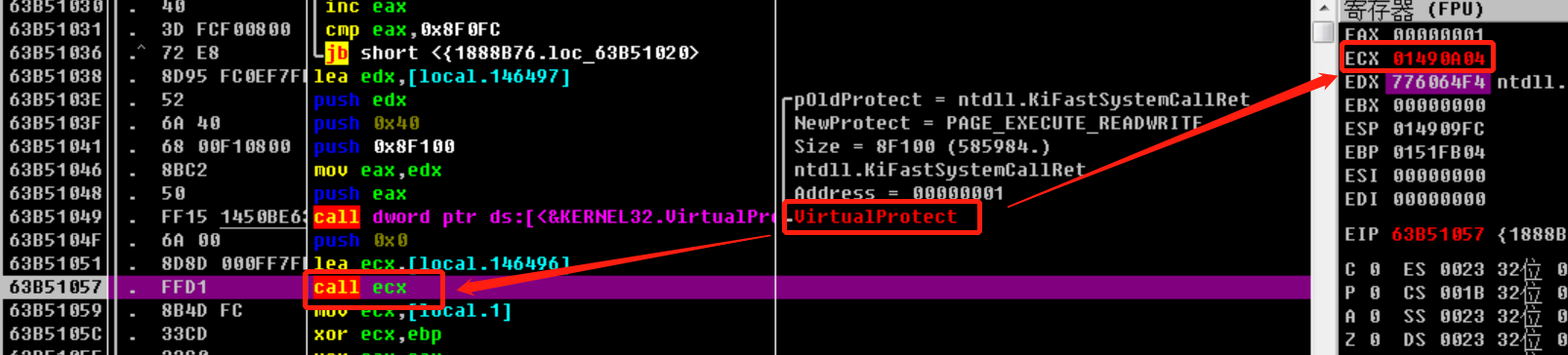


## 0x04 在0X63B51000处下段开始分析这个地址做了什么

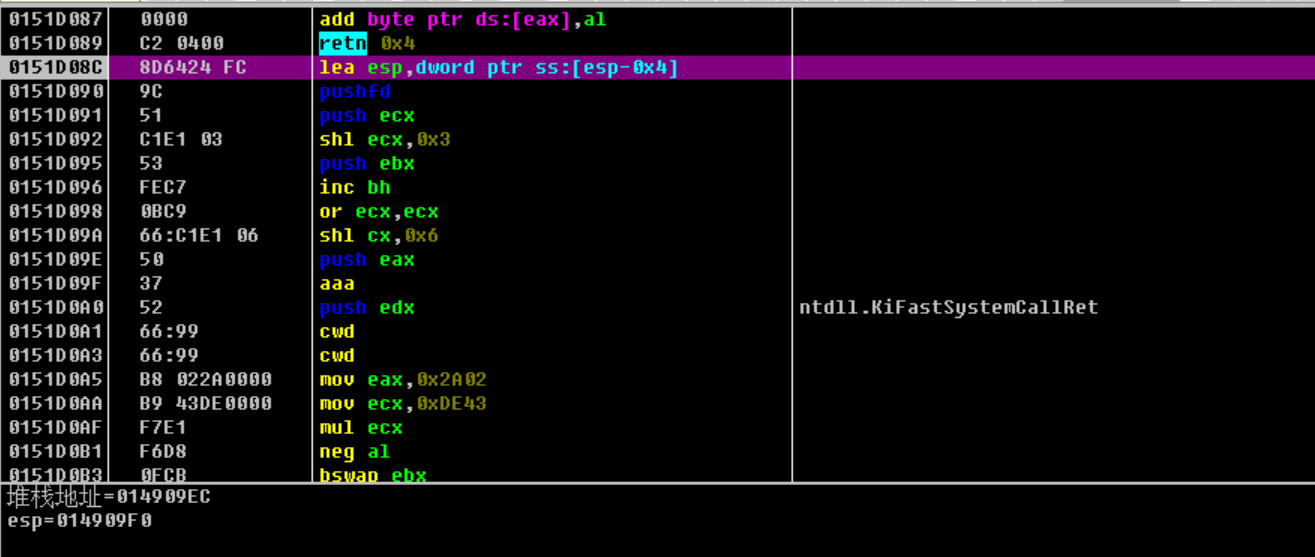
4.1 断点断下



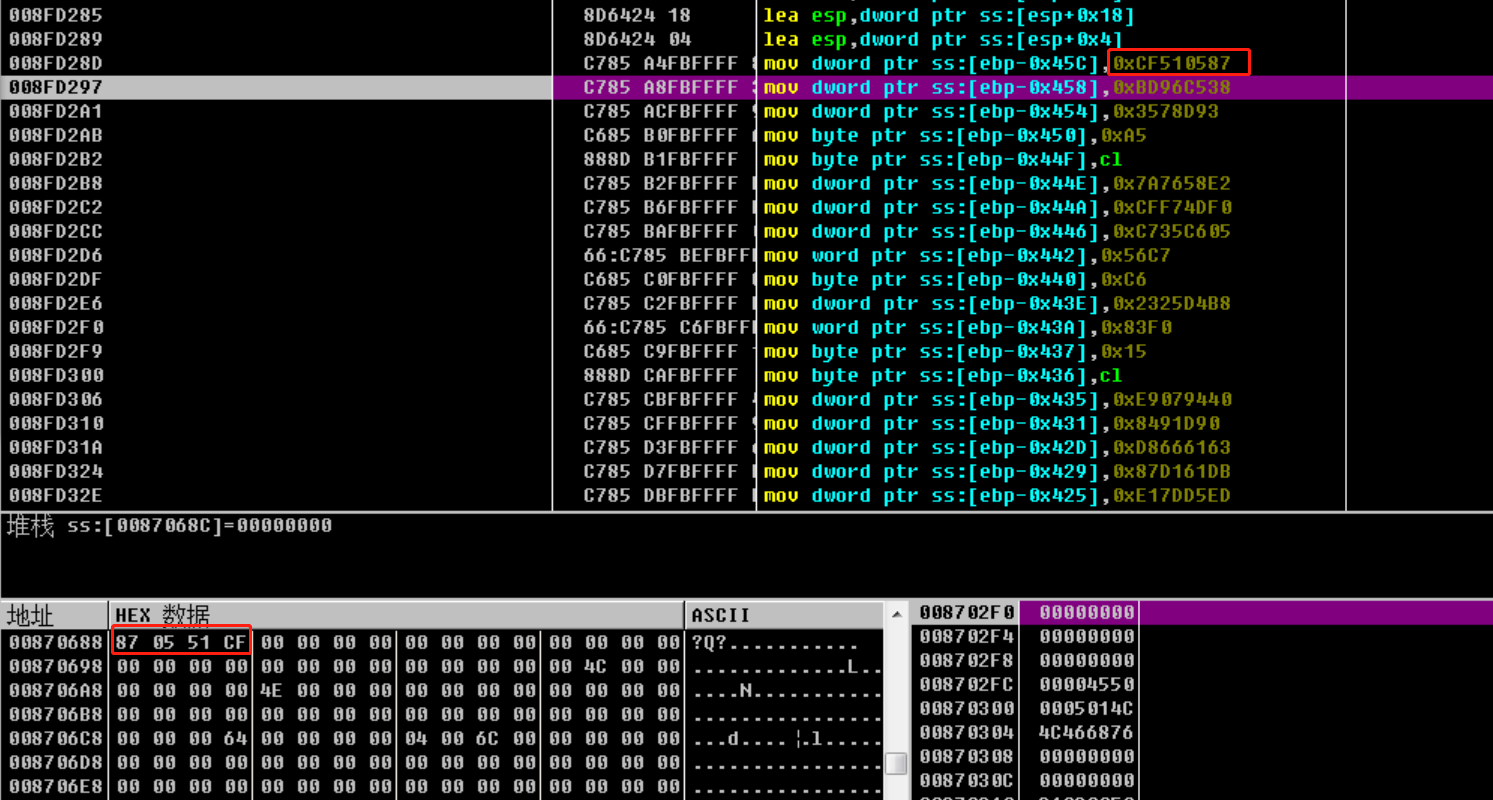
4.2 可以看到virtualprotect修改0X1490A04处的值为可读可写，然后call到这个地址开始执行。



4.3 跟进来之后发现这里面是一段无意义的指令混淆，猜测这是第一段shellcode（里面有大量的混淆指令，可以在等他解密完成之后将释放的DLL 从内存中dump出来）。

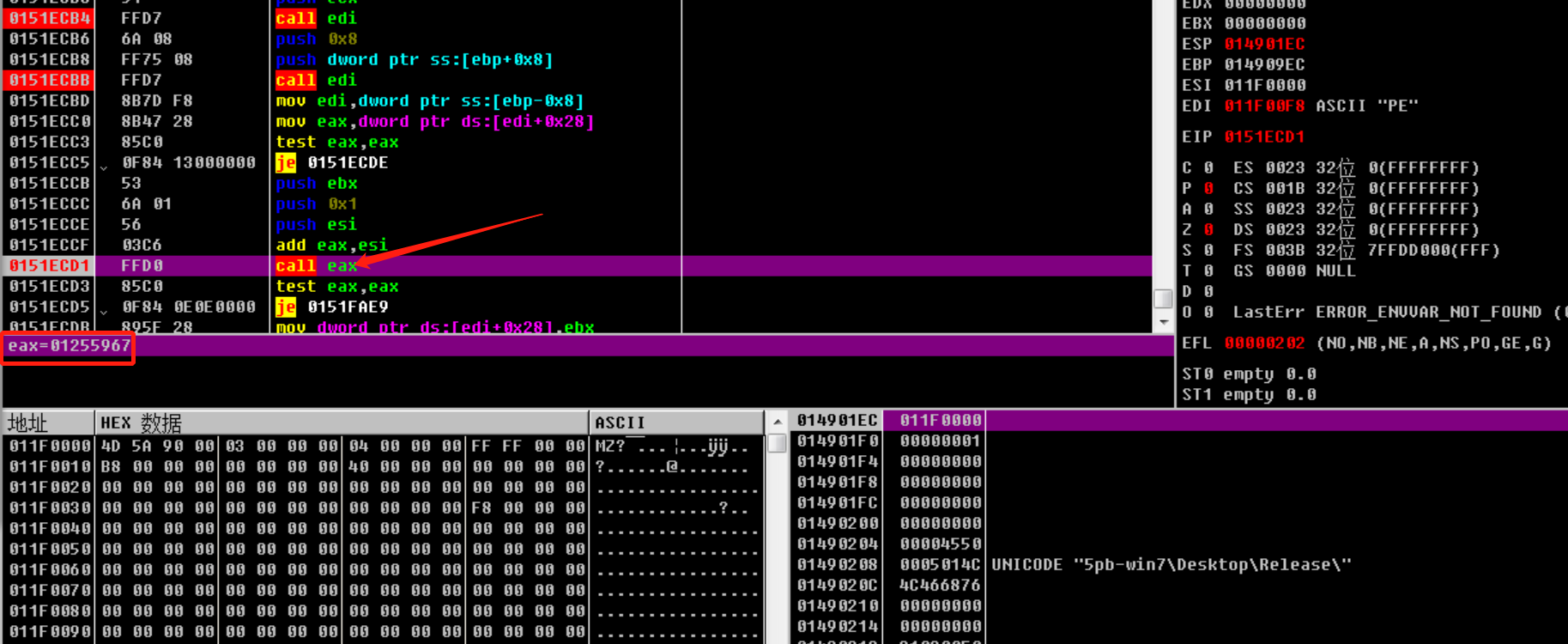


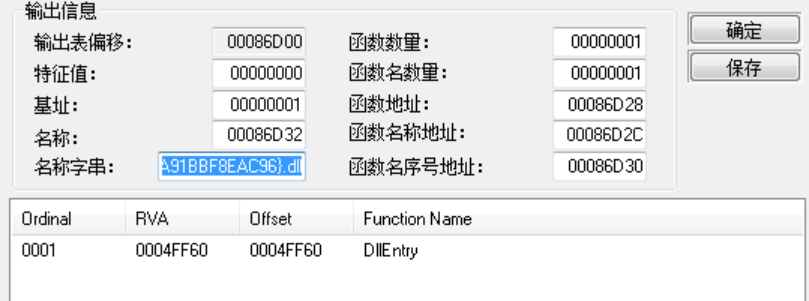
4.4 将预备的字节码写入内存



## 0X05 dump 解密后的{A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll

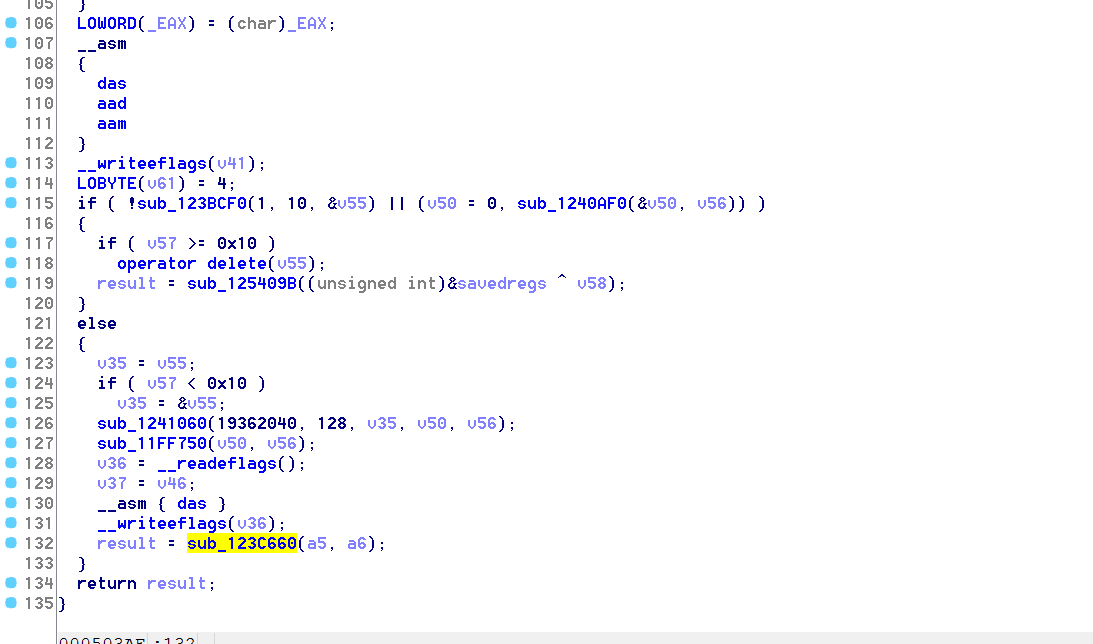
5.1 找到了第一段释放的第一段dll，{A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll





## 0X06 开始调试{A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll

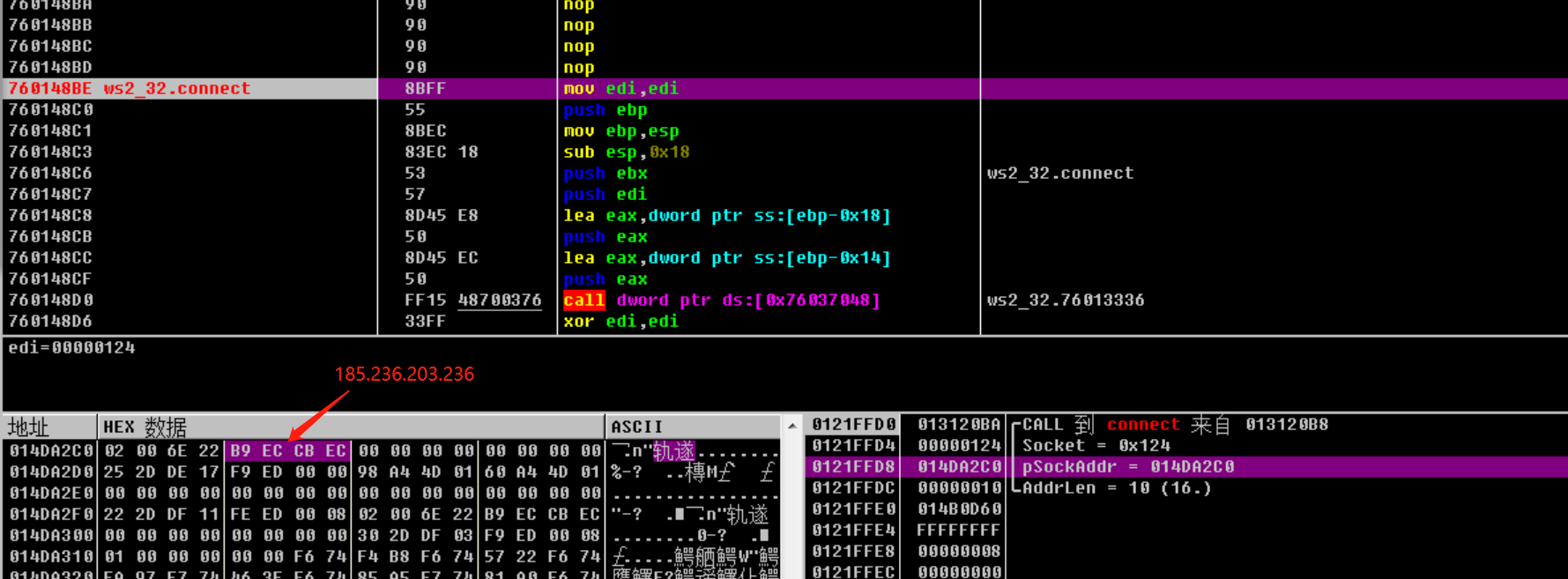
6.1 用IDA解析{A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll分析后发现，其DllEntry无特别作用，但是它提供了针对源资源的解密方法，后续的程序流程中将调用揭秘方法解密出敏感信息（如网络相关的CC）。



6.2 进入新解密出来的DLL继续往下调试，在FindResouce、LoadResouce、SleepEx、VirtualAlloc、VirtualProtect，网络连接等API下断。

02 
03 
012FBF13 
ß12FBF1 
012FBF17 
012FBF19 
012FBFIF 
012FBF20 
NULL 
"12FBF25 
012FBF28 
"12FBF2A 
012FBF2C 
012FBF32 
0.0 
012FBF33 
0.0 
012FBF38 
0.0 
912FBF3B 
0.0 
912FBFug 
0.0 
912FBF41 
0.0 
912FBF113 
0.0 
912FBF46 
0.0 
612FBF118 
912FBF11E 
012FBF51 
esi=ß133Bß8ß 
80 96 
8B5424 OC 
14 
89 
68 
FFD3 
8BFO 
85F6 
A3gggggg 
56 
68 
FF55 F8 
8BD8 
85DB 
9ggggggg 
56 
68 gogg2Bß1 
FF55 
E9 gggggggg 
53 
8BFß 
FF55 
85Cß 
8B4D 
56 
popfd 
mou edx,dword ptr 
lea 
esp,dword ptr 
mou dword ptr ,ecx 
Ox12BOOOO 
ebx 
esi ,eax 
mou 
test esi ,esi 
012FBFC2 
esi 
Ox12Bgggg 
dword ptr 
mou ebx,eax 
test ebx ,ebx 
012FBFC2 
esi 
Ox12Bgggg 
dword ptr 
012FBF40 
ebx 
esi ,eax 
nou 
eau dword ptr 
test eax,eax 
012FBFC2 
KernelBa . 
7579CA61 
kerne132 -FindResourceW 
kerne132 -LoadResource 
kerne132 -FindResourceW 
kerne132 -SizeofResource 
kerne132 -FindResourceW 
kerne132 -LockResource 
EBP 
ESI 
EDI 
EIP 
c 
P 
z 
s 
o 
EFL 
STO 
STI 
ST2 
ST3 
STI' 
STS 
ST6 
FST 
FCW 
012203E8 
01338080 
75F30000 kerne132.75F30000 
012FBF25 
ES 
cs 
DS 
FS 
GS 
0023 
go-IB 
0023 
0023 
003B 
32 
32 
32 
32 
32 
"(FFFFFFFF) 
"(FFFFFFFF) 
"(F FFFFFFF) 
"(F FFFFFFF) 
7FFDEOOO(FFF) 
LastErr 
02 
ERROR_SUCCESS 
ss:[ebp 
ecx ,dword ptr 
nou 
cc 
02 
02 
71 
78 
33 
FC 
21 
A6 
Eli 
53 
CA 
El 
-oxlß] 
0122ß3C11 
0122ß3C8 
012203cc 
0122ß3Dß 
012203D8 
012203DC 
0122ß3Eß 
empty 
emp ty 
emp ty 
emp ty 
emp ty 
emp ty 
emp ty 
emp ty 
027F 
3210 
NEAR , 53 
ESP 
Err g 
Cond 
Prec 
0133B 08 g 
0133B 09 g 
0133B gag 
0133B OBO 
0133B OCO 
0133B ODO 
0133B OEO 
HEX 
cc 
79 
78 
26 
08 
98 
F5 
86 
63 
15 
71 
69 
23 
53 
119 
8B 
esi 
ASCII 
yH1 
FC 
ID 
8F 
12 
El 
012BOOOO 
0133B 08 0 
ßßßßßßßß 
ßßßßßßßß 
ßßßßßßßß 
75F73115C 
75F79211D 
75F7D3BO 
kernel 32 . LockResource 
kernel 32 . SizeofResource 
kerne132. LoadResource 

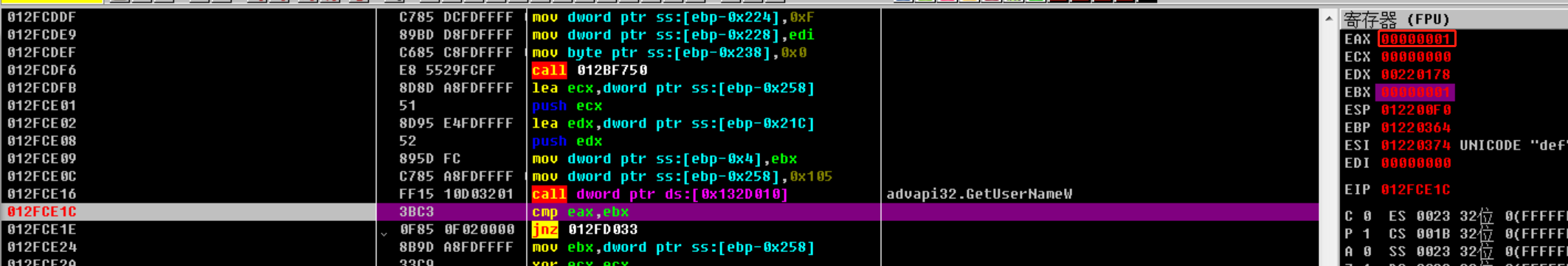
看到程序找到资源文件位置并将其加载，并获取资源的大小和指针。



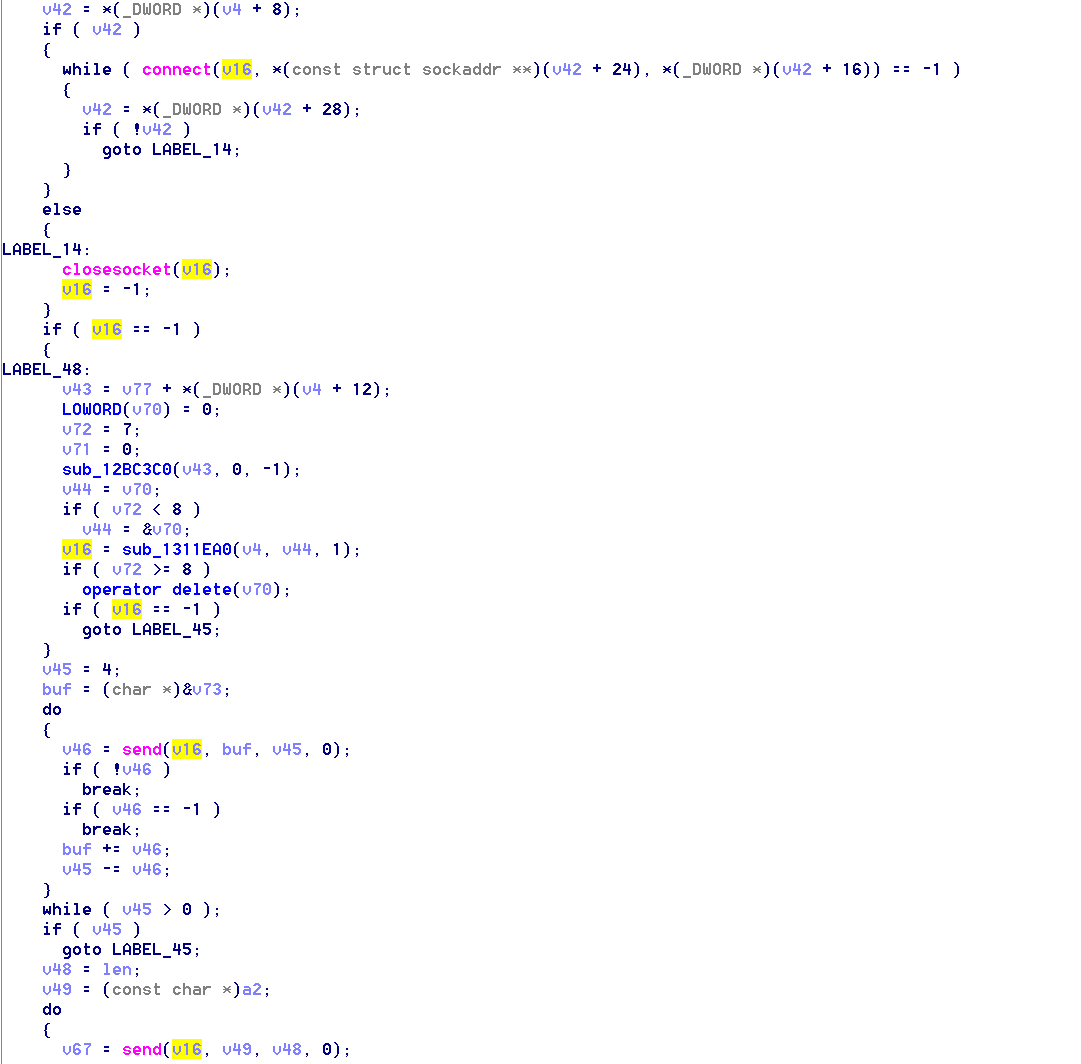
与海莲花的IP建立链接

"986245B 
ggB6245F 
69862463 
698621171 
698621176 
698621179 
ßßB62U7E 
eax=ßßC7FD91' 
HEX 
66:89 
8DUD C 
8845 c 
BE 98 
3975 
mou 
lea 
mou 
mou 
mou 
mou 
c mp 
word ptr 
eax 
,dword 
dword ptr 
dword ptr 
ggegcacg 
,dword 
esi , 
dword ptr 
ptr 
ss:[ebp 
ss:[ebp 
-gx2ß] , 
-gx24] 
bp-gxu 
(UNICODE 
01 
48 
35 
37 
3B 
"ad.ssageeurenue-com") 
ASCII 
ßßEC6BU8 
ggEC6B58 
ggEC6B68 
ßßEC6B78 
ggEC6B88 
ggEC6B98 
92 
22 
01 
92 
32 
36 
39 
3B 
73 
75 
75 
75 
75 
19 
3B 
75 
75 
75 
EC 
75 
75 
75 
75 
35 
38 
3B 
EC 
75 
75 
75 
75 
'6uo....@7uoP8uo 
;uo 
ßßC7FD68 
ßßC7FD6C 
ßßC7FD7ß 
ßßC7FD71' 
ßßC7FD78 
ßßC7FD7C 
ßßC7FD8ß 
gggggggg 
ßßD214B8 
gggggggg 
gggggggg 
ggggggg2 
gggggggl 
ggggggg6 

获取海莲花的域名

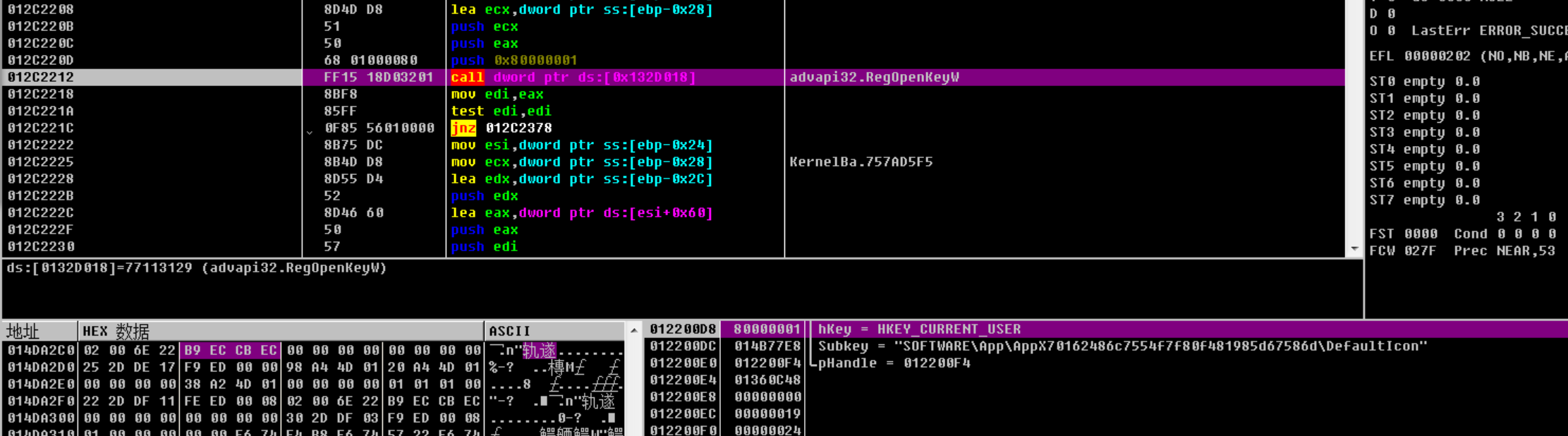


成功获取用户名



ßßB6267F 
ggB6268ß 
69862681 
69862682 
69862688 
69862689 
ggB6269ß 
69862693 
69862699 
6986269B 
ggB6269D 
ggB6269F 
"3F73ß8 
"3F7318 
"3F7328 
"3F7338 
ßß3F7348 
"3F7358 
( ws2 
5B 
85cg 
83F8 
"3D8 
ßF8F 
35 
esl 
edi 
call 
60862695 
c mp 
60862695 
sub 
add 
ßßB6267D 
HEX 
5B 
68 
13 
75 
75 
11 
46 
35 
27 
82 
67 
32 -send) 
46 
88 
65 
98 
93 
ASCII 
39 
80 . ......T$5 
ßßC7FD5C 
ßßC7FD6ß 
ßßC7FD61' 
ßßC7FD68 
ßßC7FD6C 
ßßC7FD7ß 
goggß188 
"3F73ß8 
goggßß19 
gggggggg 
gggggggg 
ßßD214B8 
gggggggg 
Socket - 
gx188 
Data - 
"3F73ß8 
DataSize - 
Flags 

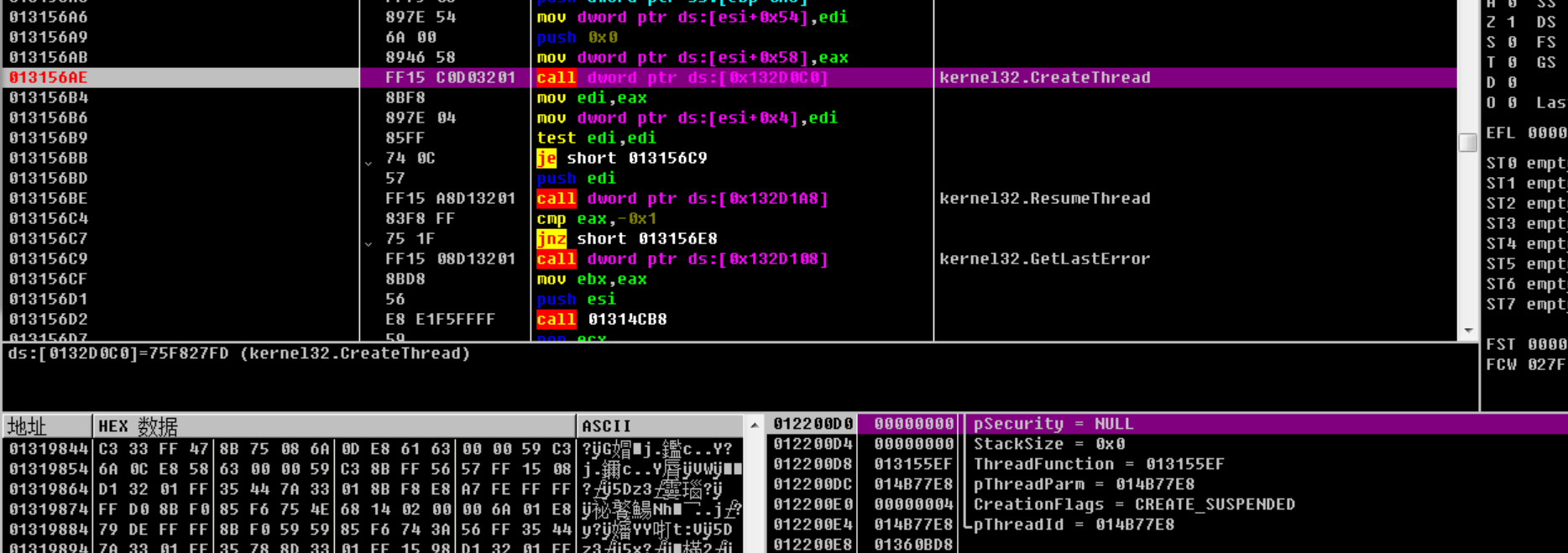
建立socket连接并发送消息



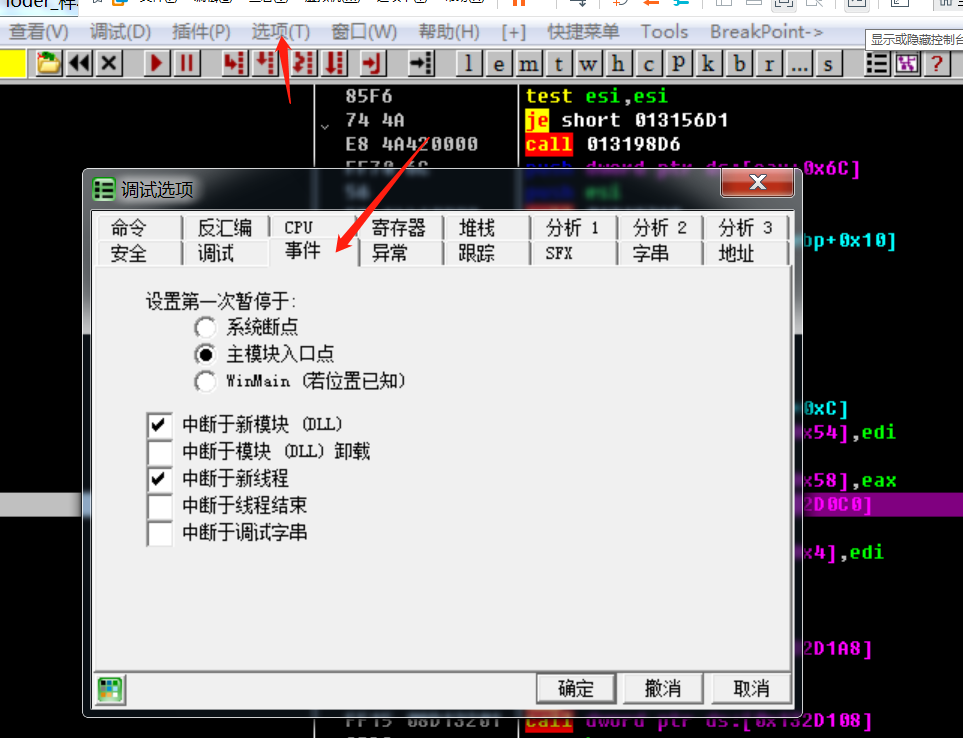
打开注册表

HKEY\_CURRENT\_USER\Software\App\AppX70162486c7554f7f80f481985d67586d\DefaultIcon

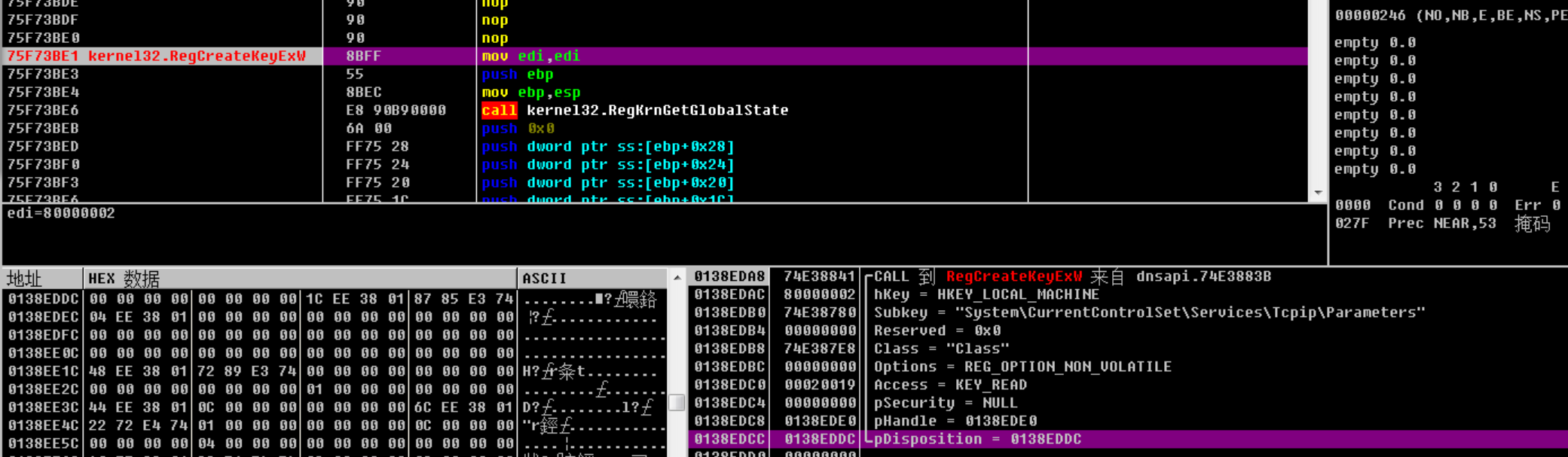




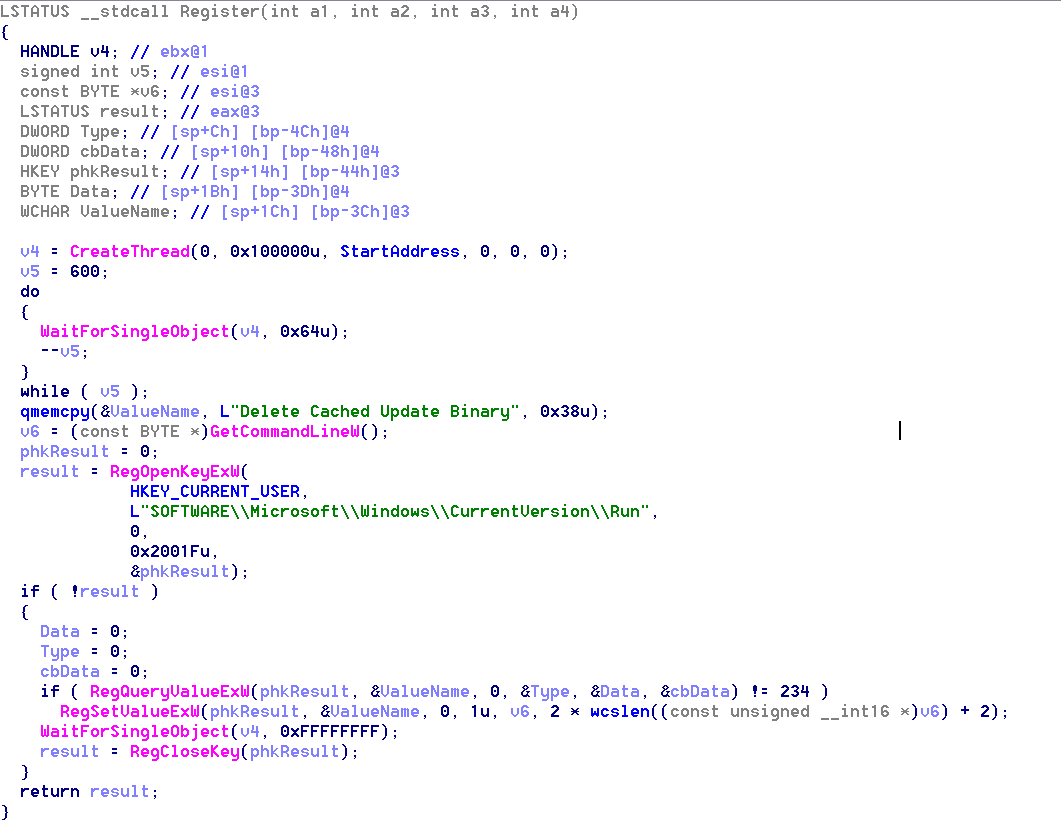
以挂起的方式创建线程，之后需要的时候用ResumeThread恢复线程运行。

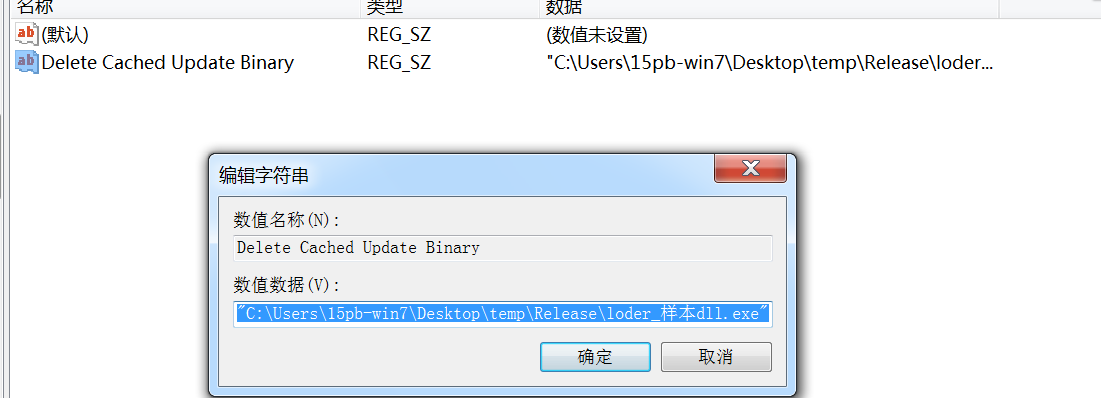


我们在这里可以设置调试器中断于新的线程。

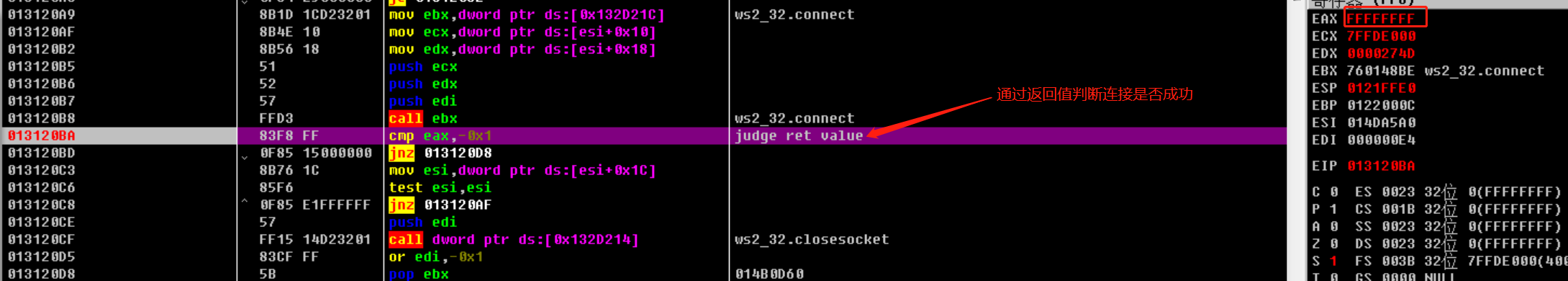


设置TCPIP链接注册表键





设置注册表键值添加自启动项



之后会根据connect的返回值来判断是否链接成功，返回-1表示链接失败，因为这个IP已经无法链接了所以我们可以把返回值手动修改为0，能看到后续执行了send函数发送数据。

ßßB6267D 
ßßB6267F 
ggB6268ß 
69862681 
69862682 
69862688 
69862689 
ggB6269ß 
69862693 
69862699 
6986269B 
ggB6269D 
ggB6269F 
hu?.ä$?........ 
esl 
edi 
60862695 
c mp 
60862695 
sub 
add 
ßßB6267D 
( ws2 
CD 
73 
32 -send) 
"3F73ß8 
"3F7318 
"3F7328 
"3F7338 
ßß3F7348 
"3F7358 
HEX 
91 
5B 
68 
CD 
85cg 
83F8 
"3D8 
ßF8F 
35 
73 
56 
41 
35 
01 
ASCII 
65 
88 ...T$5 
Socket - 
gx188 
Data - 
"3F73ß8 
DataSize - 
Flags 
39 
67 
18 
88 
75 
38 
46 
88 
75 
ßßC7FD5C 
ßßC7FD6ß 
ßßC7FD61' 
ßßC7FD68 
ßßC7FD6C 
ßßC7FD7ß 
goggß188 
"3F73ß8 
goggßß1F 
gggggggg 
gggggggg 
ßßD214B8 
gggggggg 

0X07 IOC

网络C2

|  |  |
| --- | --- |
| 回连域名 | us.melvillepitcairn.com  sys.genevrebreinl.com  ad.ssageevrenue.com  tel.caitlynwells.com |

释放文件及中间件哈希

|  |  |
| --- | --- |
| 文件名 | MD5 |
| {1888B763-A56C-4D4B-895C-2092993ECCBA}.dll | DADE969B00CBC4A0C1B58EEB0E740B63 |
| 渔政大队2019年安全生产执法检查工作总结.docx | DC4DBB375615657D1006666452382AB1 |
| {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll | FD0535A73AD63FA83326C2D8295DB94B |

0X08 总结

此海莲花样本选用了伪装成word文件图标的.exe文件，在木马运行过程中无文件落地，解密的shellcode存在较多的加密混淆操作，后续的窃密远控行为分为多线程执行，其执行流程在多模块间跳转，在一定程度上加大了逆向分析的难度。总的来说该样本具有较强的隐蔽性和较高的稳定性。