Polymorphic virus deformation characteristics in the application of encryption

Zhong Fangtian, Zhu Hao

Northeast normal university,Changchun,JiLin,China

zhongft496@nenu.edu.cn, zhuh102@nenu.edu.cn

Keywords: software encryption,polymorphic decryption,reverse crack

ABSTACT : In recent years, the software development industry are developed rapidly with the development of software and hardware technology and the rapid expansion of the number of users.At the same time, the software encryption technology and the technique of reverse analysis also gradually narrowed, the fight for the sake of illegally obtaining the right to use the software and a better user experience. Software is illegal to shorten the running period, in this paper, the author will ensure software are proposed according to the deformation characteristics of polymorphic decryption module of the randomness of encryption technology, reverse engineer, reverse crack technology to increase the difficulty and time cost, better protection software property rights, maintain the normal operation of the software cycle.

Introduction

Software encryption and reverse crack is a confrontational technology, many developers because of the lack of understanding of decryption, causing them to spend a lot of manpower and final design out the protection of vulnerable, therefore, the industry developed some professional protection program (also known as shell), [1]Such as UPX, ASPack, PECompact compression shell and ASProtect, Armadillo, pangolin scales, EXECryptor, Themida encryption shell, of course, powerful VMProtect virtual machine protection technology, however, even if is encrypted, the tracking code, CRC check, use Blowfish, Twofish, TEA and other powerful encryption algorithm ASProtect encryption shell, reverse engineer use OllyDbg this powerful dynamic debugger combines LoadPE reconstruction to the powerful features of the input table can find the OEP, ASProtect shell off; Use OllyDbg dynamic debugging function according to the principle of balance of stack, thus find the OEP removal program UPX,[2] PECompact compression shell;Due to the protective mechanism of VMProtect virtual machine protection technology is the original X86 assembly made according to the program defined by a set of instruction system is explained by the corresponding bytes into PE executable file pattern, and delete the original X86 assembly instruction, finally in program execution is interpreted by a virtual machine when starting, but often a assembly instruction after processing to the corresponding bytecode VM can expand several times or even one hundred times, this will seriously affect the efficiency of the execution of the program, combined with VMProtect virtual machine protection technology of high technical threshold so that its failure to widely used; the program were randomly selected in each run different decryption decryption module that has been encrypted code execution,[3] bitlocker can increase the types of decryption module to add reverse crackers reverse analysis of the amount of time cost and increase the complexity of the decryption modules to enhance difficulty so as to better protect software reverse analysis.

The Deformation Principle Of Metamorphic Viruses

Deformation technology originated in the encryption technology, the early of the virus to evade antivirus software to virus signature scanning, main body of the virus body by traditional encryption technology encryption protection, when the virus is triggered, the virus first execute and perform the decryption decryption module to virus subject, but this kind of virus in the encryption protection technology has fixed the decryption module, which makes the antivirus software can be based on the characteristics of decryption module testing of killing, in the process of deformation in order to overcome the traditional encryption technology (decryption module characteristic testing), polymorphic transformation technique is widely used, in order to make the decryption module after each virus infection presents different structure forms, Polymorphic deformation technology USES engine to deformation protection of decryption module, in does not affect the code execution logic function, under the condition of deformation engines often by changing the instruction execution order, equivalent instructions to replace, the development of instruction, and compression and random insertion technique such as garbage instructions and flowers to deformation protection of decryption module code, deformation of engine model is shown in figure 1.

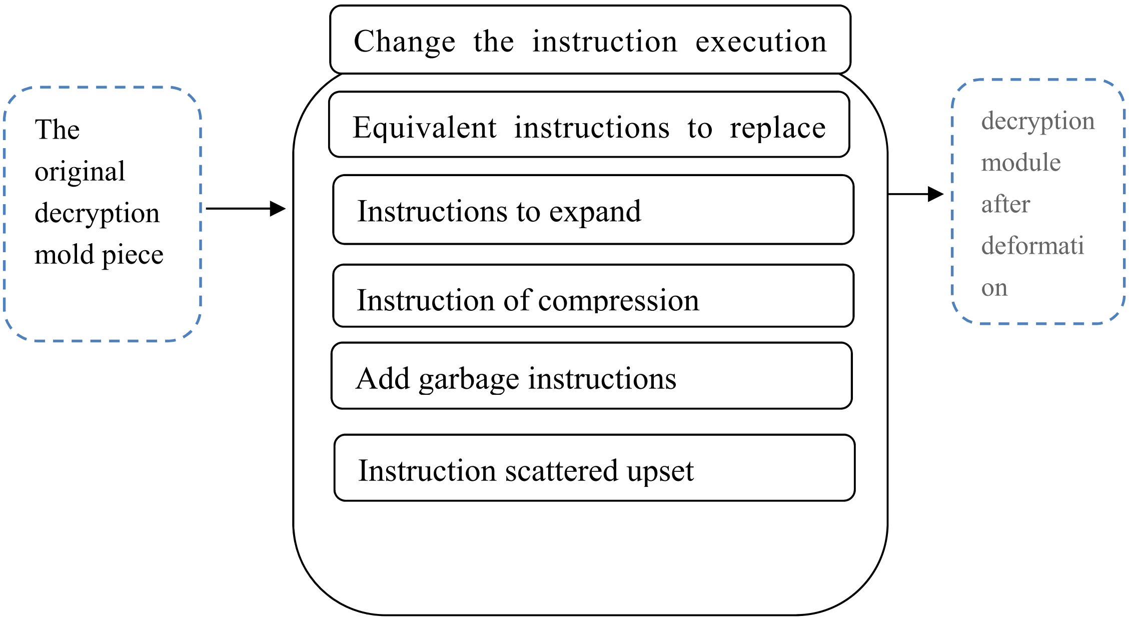
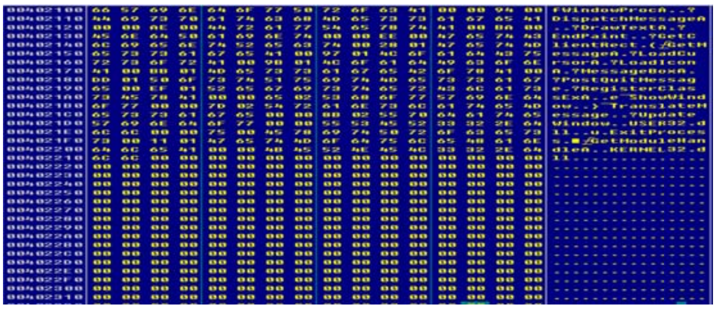

The original decryption mold piece
Change the instruction execution
Equivalent instructions to replace
Instructions to expand
Instruction of compression
Add garbage instructions
Instruction scattered upset
decryption module after deformati on

Fig. 1. deformation of engine model

as shown in figure 2, to a greater degree of changing the structure of the decryption module configuration, deformation engine decryption module can be broken down into different specifications of a code block, then these small code layout to PE alignment block in the blank area, at the same time, by inserting a large number of JMP instruction to maintain its execution logic, to ensure that the results of execution; PE file alignment blocks of empty area:



```
00402100 66 57 69 6E 64 6F 77 50 72 6F 63 41 00 00 94 00 fWindowProcA..?
00402110 44 69 73 70 61 74 63 68 4D 65 73 73 61 67 65 41 DispatchMessageA
00402120 00 00 AE 00 44 72 61 77 54 65 78 74 41 00 BA 00 ..?DrawTextA.?
00402130 45 6E 64 50 61 69 6E 74 00 00 EE 00 47 65 74 43 EndPaint..?GetC
00402140 6C 69 65 6E 74 52 65 63 74 00 28 01 47 65 74 4D lientRect.(┌GetM
00402150 65 73 73 61 67 65 41 00 97 01 4C 6F 61 64 43 75 essageA.?LoadCu
00402160 72 73 6F 72 41 00 9B 01 4C 6F 61 64 49 63 6F 6E rsorA.?LoadIcon
00402170 41 00 BB 01 4D 65 73 73 61 67 65 42 6F 78 41 00 A.?MessageBoxA.
00402180 DD 01 50 6F 73 74 51 75 69 74 4D 65 73 73 61 67 ?PostQuitMessag
00402190 65 00 EF 01 52 65 67 69 73 74 65 72 43 6C 61 73 e.?RegisterClas
004021A0 73 45 78 41 00 00 65 02 53 68 6F 77 57 69 6E 64 sExA..e¯ShowWind
004021B0 6F 77 00 00 7D 02 54 72 61 6E 73 6C 61 74 65 4D ow..}¯TranslateM
004021C0 65 73 73 61 67 65 00 00 8B 02 55 70 64 61 74 65 essage..?Update
004021D0 57 69 6E 64 6F 77 00 00 55 53 45 52 33 32 2E 64 Window..USER32.d
004021E0 6C 6C 00 00 75 00 45 78 69 74 50 72 6F 63 65 73 ll..u.ExitProces
004021F0 73 00 11 01 47 65 74 4D 6F 64 75 6C 65 48 61 6E s.■┌GetModuleHan
00402200 64 6C 65 41 00 00 4B 45 52 4E 45 4C 33 32 2E 64 dleA..KERNEL32.d
00402210 6C 6C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ll..............
00402220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00402230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00402240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00402250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00402260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00402270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00402280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00402290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
004022A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
004022B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
004022C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
004022D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
004022E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
004022F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00402300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00402310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

Fig.2 Decryption module configuration

Polymorphic Deformation Characteristics In The Application Of Encryption Scheme

Using the deformation of metamorphic engine principle of software encryption to protect the key code in the process of the adjustment of the instruction execution order, instructions of compression, [6]the development of instruction, and equivalent substitution as well as add garbage processing instructions and flowers such as deformation, make through deformation processing module can hardly be reverse engineer the debug analysis, using the deformation principle of virus, the author will put forward a new kind of concrete implementation plan, as shown in figure 3

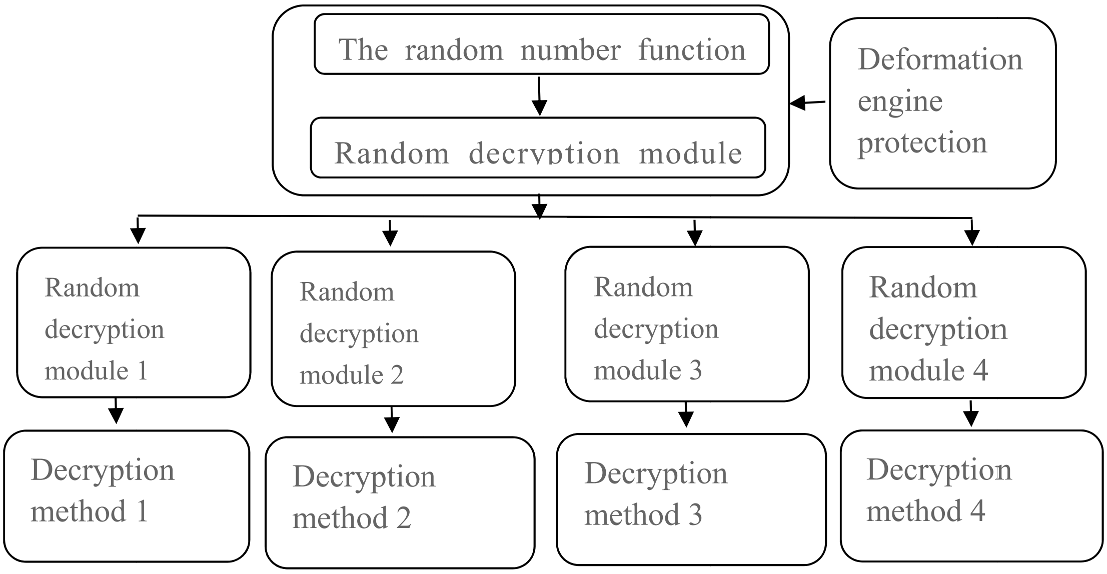

The random number function
Random decryption module
Deformation engine protection
Random decryption module 1
Random decryption module 2
Random decryption module 3
Random decryption module 4
Decryption method 1
Decryption method 2
Decryption method 3
Decryption method 4

Fig.3 Concrete implementation plan

As shown in figure 3, the program will first perform a random function, according to the generated random number and decryption module address to find the relation between the corresponding decryption module address, [7]And then execute the corresponding decryption module of a program has encryption module (program validation process) decryption, access to verify whether the user has a procedure or function access, etc., but it and general encryption program did not have any distinction, according to the binary code in the disassemble of assembler, whether API function provided by the system itself, or user defined function is through the EAX storage function return values, So only need to reverse engineer in OllyDbg or IDA debugging tools such as modified by means of Patch EAX as a fixed value, random function returns a value to a constant value, the program can only perform a fixed way of decryption, and of other ways to decrypt,it doesn't make any sense, however, use of metamorphic engine technology to generate random Numbers and random decryption module in the program address block of code that are not protected, because after deformation engine with a block of code will present a completely different morphological structure, each has the characteristics of not debugging, the distortion after engine deformation processing, assurance procedures generate random Numbers and random secret module address block of code that effective, Each time the program execution method is also adopted by the completely random, so the software reverse engineer to reverse crack, must be on each and find a way to decrypt the reverse analysis method of crack, the application of encryption protector if you want to increase the difficulty of reverse engineer the reverse crack, on the one hand, can increase the difficulty that the decryption module algorithm, on the other hand can increase the number of decryption module,[8] different from the traditional way of application protection, can only use one way to decrypt has encryption module, the use of the way a virus deformation engine protection will ensure applications have multiple protection methods at the same time, at the same time, this kind of protection way can expand sex is very strong, so no matter how much each way of decryption decryption module is simple, when the number of decryption module reaches a certain extent, to reverse engineer the reverse break the amount of time the price is hard to imagine, unless the application has enough value.

New Type Of Decryption Module

Here the author will put forward a kind of new way called overlay decryption, as shown in figure 4

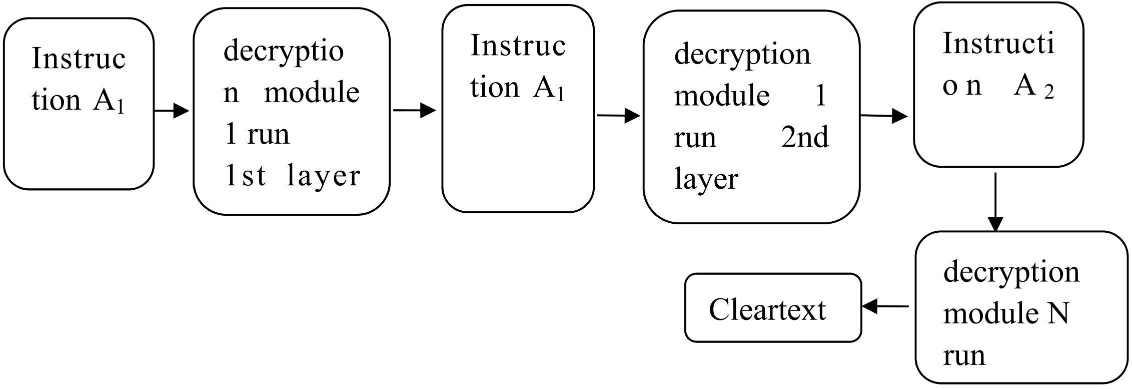
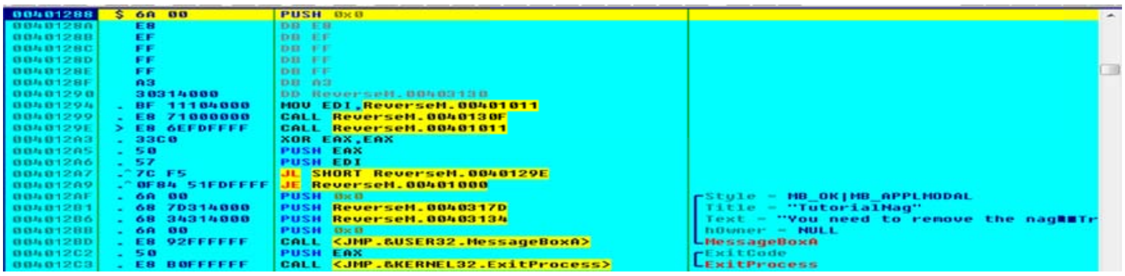


Fig. 4 A new way called overlay decryption

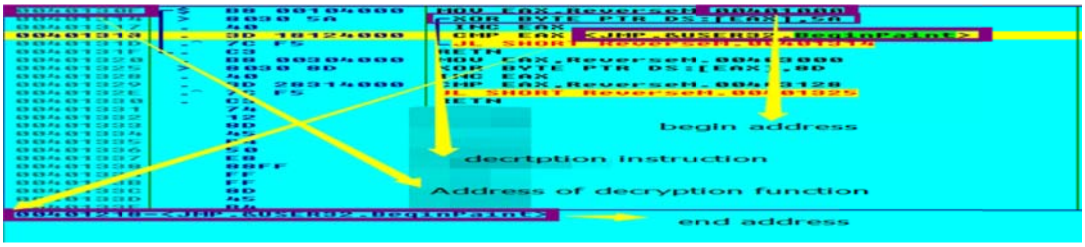
Different from the traditional way of decryption decryption module only has encryption to protect the code for a decryption can get final clear code, as shown in figure 4, the author put forward the decryption mode for the same memory address has encryption to protect any instructions to the declassification of more than one can obtain the final executable proclaimed in writing code, using the overlay decryption method of decryption encryption module, want to reverse engineer the reverse crack must clear the reverse out each layer encryption keys to find the corresponding public key, but it is far from enough, as a result of what use is to the same memory address instructions covering decryption model, so the reverse engineer must also consider each layer is brought about by the knock-on effect when the Patch, Consider this cover type when decryption decryption module layer reaches a certain magnitude, its theory is not to crack, then the author through an experiment using quadratic decryption program interpretation overlay decryption technology, laboratory application binary disassembly code as shown below:



```
00401288  $ 6A 00           PUSH 0x0
0040128A    E8              DB E8
0040128B    EF              DB EF
0040128C    FF              DB FF
0040128D    FF              DB FF
0040128E    FF              DB FF
0040128F    A3              DB A3
00401290    30314000        DD ReverseM.00403130
00401294  . BF 11104000     MOV EDI,ReverseM.00401011
00401299  . E8 71000000     CALL ReverseM.0040130F
0040129E  > E8 6EFDFFFF     CALL ReverseM.00401011
004012A3  . 33C0            XOR EAX,EAX
004012A5  . 50              PUSH EAX
004012A6  . 57              PUSH EDI
004012A7  .^7C F5           JL SHORT ReverseM.0040129E
004012A9  .^0F84 51FDFFFF   JE ReverseM.00401000
004012AF  . 6A 00           PUSH 0x0                                   ┌Style = MB_OK|MB_APPLMODAL
004012B1  . 68 7D314000     PUSH ReverseM.0040317D                     │Title = "TutorialNag"
004012B6  . 68 34314000     PUSH ReverseM.00403134                     │Text = "You need to remove the nag■■Tr
004012BB  . 6A 00           PUSH 0x0                                   │hOwner = NULL
004012BD  . E8 92FFFFFF     CALL <JMP.&USER32.MessageBoxA>             └MessageBoxA
004012C2  . 50              PUSH EAX                                   ┌ExitCode
004012C3  . E8 B0FFFFFF     CALL <JMP.&KERNEL32.ExitProcess>           └ExitProcess
```

Fig. 5

You can see in the virtual address of 00401299 and 0040129 e, there are two CALL (function CALL, the called function virtual address 0040130 f and 00401011, respectively), follow up 0040103 f function as shown in the following address:



```
MOV EAX,ReverseM.00401000
XOR BYTE PTR DS:[EAX],5A
INC EAX
CMP EAX,<JMP.&USER32.BeginPaint>
JL SHORT ReverseM.00401314
RETN
MOV EAX,ReverseM.00403000
XOR BYTE PTR DS:[EAX],8D
INC EAX
CMP EAX,ReverseM.00403128
JL SHORT ReverseM.00401325
RETN
00401218=<JMP.&USER32.BeginPaint>
```

begin address

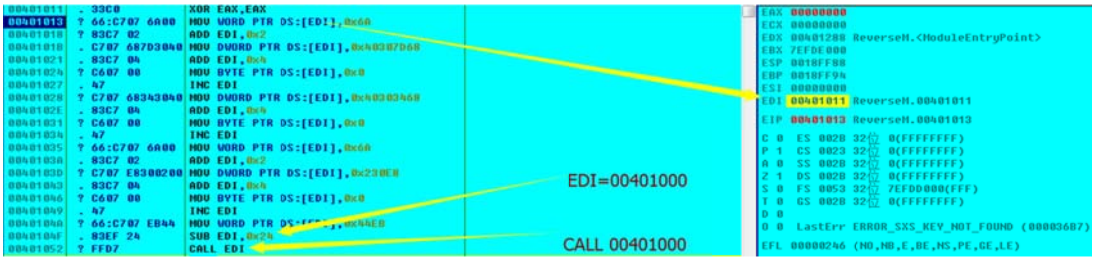
decrtption instruction

Address of decryption function

end address

Fig. 6

From the program execution logic can precipitate the the function is virtual address to a virtual address 00401000 to 00401218 block of code that contains (00401011 to 00401024) and 0 x5a exclusive or operation in bytes (for the first layer decryption operation), then follow up 00401011 address of a subroutine is as follows:



```
00401011  . 33C0            XOR EAX,EAX
00401013  ? 66:C707 6A00    MOV WORD PTR DS:[EDI],0x6A
00401018  ? 83C7 02         ADD EDI,0x2
0040101B  . C707 687D3040   MOV DWORD PTR DS:[EDI],0x40307D68
00401021  . 83C7 04         ADD EDI,0x4
00401024  ? C607 00         MOV BYTE PTR DS:[EDI],0x0
00401027  . 47              INC EDI
00401028  ? C707 68343040   MOV DWORD PTR DS:[EDI],0x40303468
0040102E  . 83C7 04         ADD EDI,0x4
00401031  ? C607 00         MOV BYTE PTR DS:[EDI],0x0
00401034  . 47              INC EDI
00401035  ? 66:C707 6A00    MOV WORD PTR DS:[EDI],0x6A
0040103A  . 83C7 02         ADD EDI,0x2
0040103D  ? C707 E8300200   MOV DWORD PTR DS:[EDI],0x230E8
00401043  . 83C7 04         ADD EDI,0x4
00401046  ? C607 00         MOV BYTE PTR DS:[EDI],0x0
00401049  . 47              INC EDI
0040104A  ? 66:C707 EB44    MOV WORD PTR DS:[EDI],0x44EB
0040104F  . 83EF 24         SUB EDI,0x24
00401052  ? FFD7            CALL EDI
```

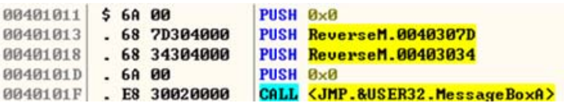
```
EAX 00000000
ECX 00000000
EDX 00401288 ReverseM.<ModuleEntryPoint>
EBX 7EFDE000
ESP 0018FF88
EBP 0018FF94
ESI 00000000
EDI 00401011 ReverseM.00401011

EIP 00401013 ReverseM.00401013

C 0  ES 002B 32位 0(FFFFFFFF)
P 1  CS 0023 32位 0(FFFFFFFF)
A 0  SS 002B 32位 0(FFFFFFFF)
Z 1  DS 002B 32位 0(FFFFFFFF)
S 0  FS 0053 32位 7EFDD000(FFF)
T 0  GS 002B 32位 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SXS_KEY_NOT_FOUND (00003687)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
```

EDI=00401000

CALL 00401000

Fig. 7

In OllyDbg dynamic tracing which function is the function of virtual address found 00401011 to 00401024 on the second floor,[8] when finish the second decryption, we will find that in 00401011 to 0040101 d virtual address in the address block a MessageBox API function, as shown



```
00401011  $ 6A 00         PUSH 0x0
00401013  . 68 7D304000   PUSH ReverseM.0040307D
00401018  . 68 34304000   PUSH ReverseM.00403034
0040101D  . 6A 00         PUSH 0x0
0040101F  . E8 30020000   CALL <JMP.&USER32.MessageBoxA>
```

Fig. 8

Throughout the execution logic program analysis, it has twice to the same address of the instruction in the decryption to expose the final clear code, Cracker to reverse analysis of this kind of program we must reverse the decryption algorithm of each layer, at the same time also need to consider to modify the upper decryption code to decrypt the lower the knock-on effect, when the declassified layer reaches a certain number, its theory is not to reverse crack, even if you can reverse cracked and a Cracker with the amount of time the price also will be immeasurable.

Summary

using polymorphic, the deformation principle of encryption protection in the process of the program to introduce deformation engines to program the key code to protect, engine will use random each deformation in this paper the deformation technique to protect key code are deformation, that is to say, this code is encrypted protector can determine, used only in the implementation process of program execution to determine, in this kind of protection mode of application, can block any static including IDA debugger, but because of the irregularity and randomness of deformation module, [9]Cracker even use OllyDbg the powerful dynamic tracing debugger didn't help either, which makes Cracker can't be broken on the reverse analysis, in order to the introduction of the deformation of the engine is not too much influence the execution of the program efficiency, the author puts forward the protection of the scheme is not directly using the deformation of the engine, deformation and protect the decryption module, but for generating random Numbers and random decryption code address block of code that are not protected, secondly, the author proposed protection scheme can expand sex is very strong, as long as the deformation of the deformation engines absolutely effective protection, can guarantee to produce random decryption address is random, so encryption, decryption protector can increase according to the requirements of their own number of decryption algorithm module, when the decryption module decryption algorithm is big enough, this can't be cracked in theory, of course, this way of protection is a program for software security space utilization coefficient, but today's computer hardware performance can meet the requirements of software encryption protector.

References

[1]Duan gang.Encryption and decryption Beijing: electronic industry press 2007.

[2]Luo Yunbing Win32 The second version of the assembly language programming Beijing: electronic industry press 2006.

[3]LiChengyuan. The core principle of reverse engineering People's posts and telecommunications publishing house.

[4]Wang Zhenhai,WangHaifeng. In view of the polymorphic anti-virus detection engine research micro computer information 2006 .9

[5]Wang Haifeng,Xia Honglei,Sun Bing. The computer system application 2006.5

[6]Wang Hongmei,Wang Juan. Deformation of polymorphic malicious code technology research Computer and digital engineering 2008

[7]Yang Wei,Wang Hong. Based on the design and realization of DSP software can Shenyang university of technology 2006.5

[8]Qing Jie. Based on the IAT encryption of the packer 2009.6

[9]Liu Xiaodong. The research and implementation of software plus shell technology 2006.3